Microsoft.AZ-500.vFeb-2024.by.Yasi.126q

Number: AZ-500
Passing Score: 800
Time Limit: 120
File Version: 33.0

Exam Code: AZ-500
Exam Name: Microsoft Azure Security Technologies

01 - Manage identity and access

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

Litware, Inc. is a digital media company that has 500 employees in the Chicago area and 20 employees in the San Francisco area.

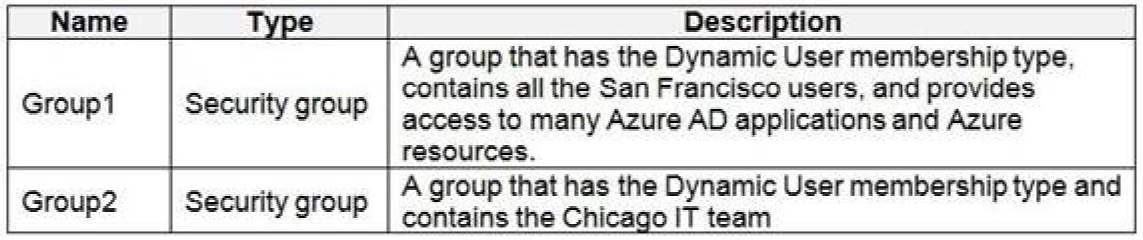
Existing Environment

Litware has an Azure subscription named Sub1 that has a subscription ID of 43894a43-17c2-4a39-8cfc-3540c2653ef4.

Sub1 is associated to an Azure Active Directory (Azure AD) tenant named litwareinc.com. The tenant contains the user objects and the device objects of all the Litware employees and their devices. Each user is assigned an Azure AD

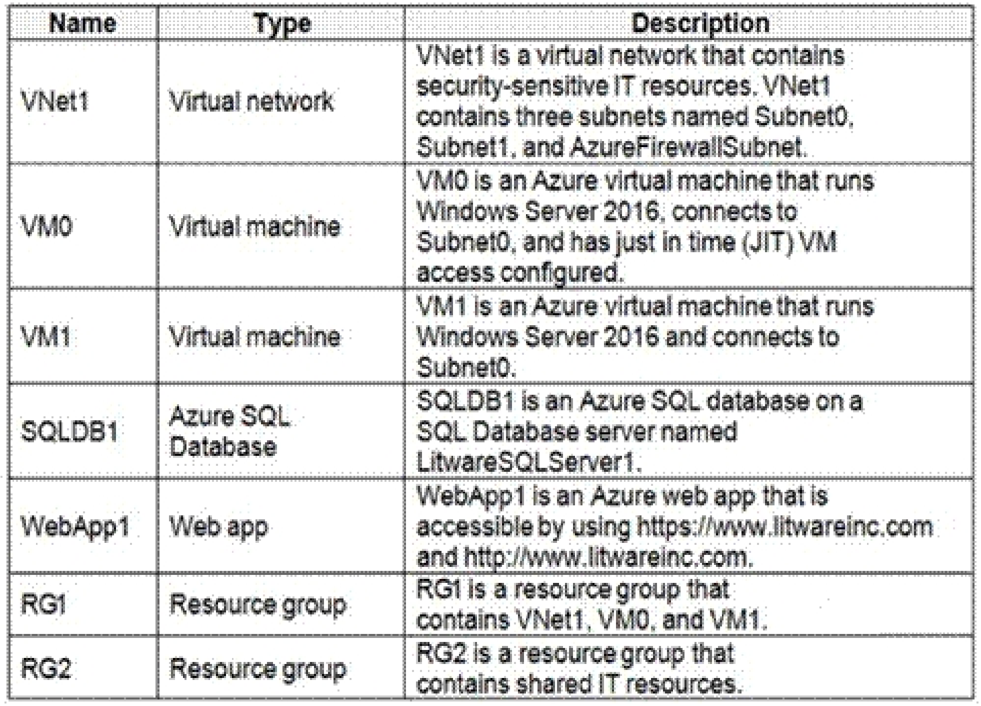
Premium P2 license. Azure AD Privileged Identity Management (PIM) is activated.

The tenant contains the groups shown in the following table.



Name	Type	Description
Group1	Security group	A group that has the Dynamic User membership type, contains all the San Francisco users, and provides access to many Azure AD applications and Azure resources.
Group2	Security group	A group that has the Dynamic User membership type and contains the Chicago IT team

The Azure subscription contains the objects shown in the following table.



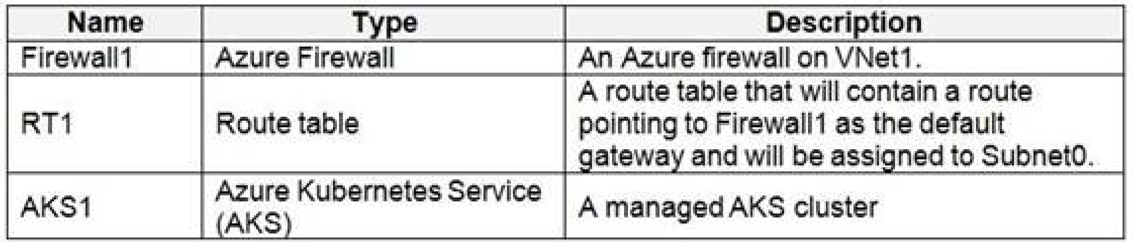
Name	Type	Description
VNet1	Virtual network	VNet1 is a virtual network that contains security-sensitive IT resources. VNet1 contains three subnets named Subnet0, Subnet1, and AzureFirewallSubnet.
VM0	Virtual machine	VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured.
VM1	Virtual machine	VM1 is an Azure virtual machine that runs Windows Server 2016 and connects to Subnet0.
SQLDB1	Azure SQL Database	SQLDB1 is an Azure SQL database on a SQL Database server named LitwareSQLServer1.
WebApp1	Web app	WebApp1 is an Azure web app that is accessible by using https://www.litwareinc.com and http://www.litwareinc.com.
RG1	Resource group	RG1 is a resource group that contains VNet1, VM0, and VM1.
RG2	Resource group	RG2 is a resource group that contains shared IT resources.

Azure Security Center is set to the Standard tier.

Requirements

Planned Changes

Litware plans to deploy the Azure resources shown in the following table.



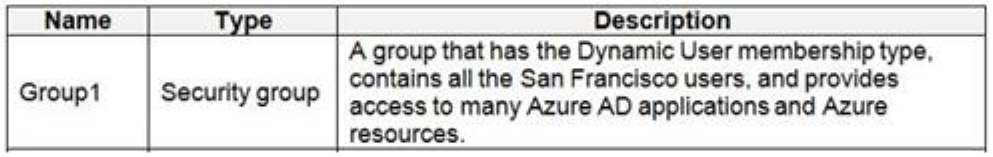
Name	Type	Description
Firewall1	Azure Firewall	An Azure firewall on VNet1.
RT1	Route table	A route table that will contain a route pointing to Firewall1 as the default gateway and will be assigned to Subnet0.
AKS1	Azure Kubernetes Service (AKS)	A managed AKS cluster

Identity and Access Requirements
Litware identifies the following identity and access requirements:
All San Francisco users and their devices must be members of Group1.
The members of Group2 must be assigned the Contributor role to RG2 by using a permanent eligible assignment.
Users must be prevented from registering applications in Azure AD and from consenting to applications that access company information on the users' behalf.
Platform Protection Requirements
Litware identifies the following platform protection requirements:
Microsoft Antimalware must be installed on the virtual machines in RG1.
The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role.
Azure AD users must be able to authenticate to AKS1 by using their Azure AD credentials.
Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access.
A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in RG1. Role1 must be available only for RG1.
Security Operations Requirements
Litware must be able to customize the operating system security configurations in Azure Security Center.
Data and Application Requirements
Litware identifies the following data and applications requirements:
The users in Group2 must be able to authenticate to SQLDB1 by using their Azure AD credentials.
WebApp1 must enforce mutual authentication.
General Requirements
Litware identifies the following general requirements:
Whenever possible, administrative effort must be minimized.
Whenever possible, use of automation must be maximized.

QUESTION 1
You need to meet the identity and access requirements for Group1.
What should you do?

A. Add a membership rule to Group1.
B. Delete Group1. Create a new group named Group1 that has a membership type of Microsoft 365. Add users and devices to the group.
C. Modify the membership rule of Group1.
D. Change the membership type of Group1 to Assigned. Create two groups that have dynamic memberships. Add the new groups to Group1.

Correct Answer: D
Section:
Explanation:
When you create dynamic groups, they can either contain users or devices. Hence here we need to create two separate dynamic groups and assign those groups to an Assigned group. Incorrect Answers:
A, C: You can create a dynamic group for devices or for users, but you can't create a rule that contains both users and devices.
D: For assigned group you can only add individual members.
Scenario:
Litware identifies the following identity and access requirements: All San Francisco users and their devices must be members of Group1.
The tenant currently contain this group:



Name	Type	Description
Group1	Security group	A group that has the Dynamic User membership type, contains all the San Francisco users, and provides access to many Azure AD applications and Azure resources.

References:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-groups-create-azure-portal

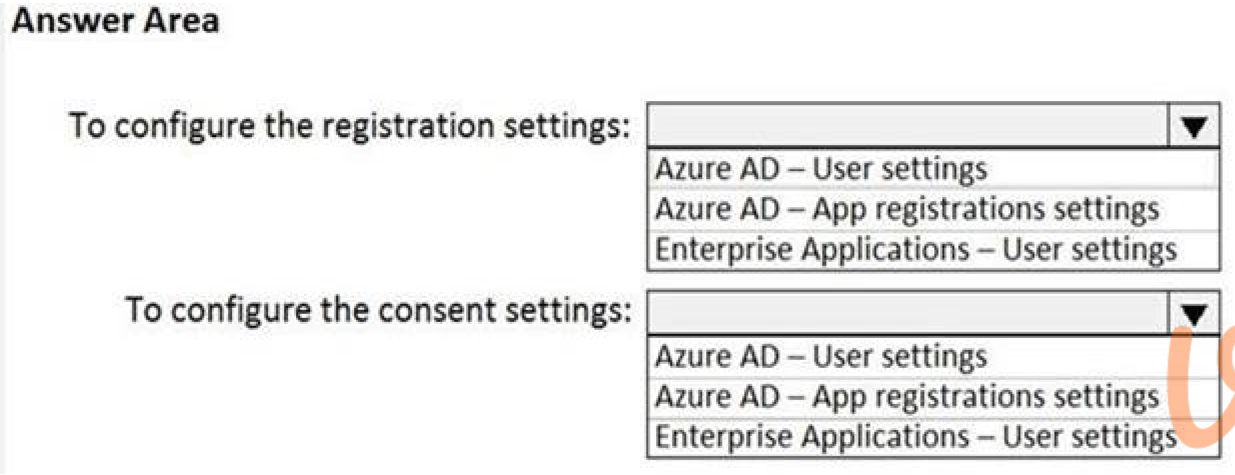
QUESTION 2

HOTSPOT

You need to ensure that the Azure AD application registration and consent configurations meet the identity and access requirements. What should you use in the Azure portal? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

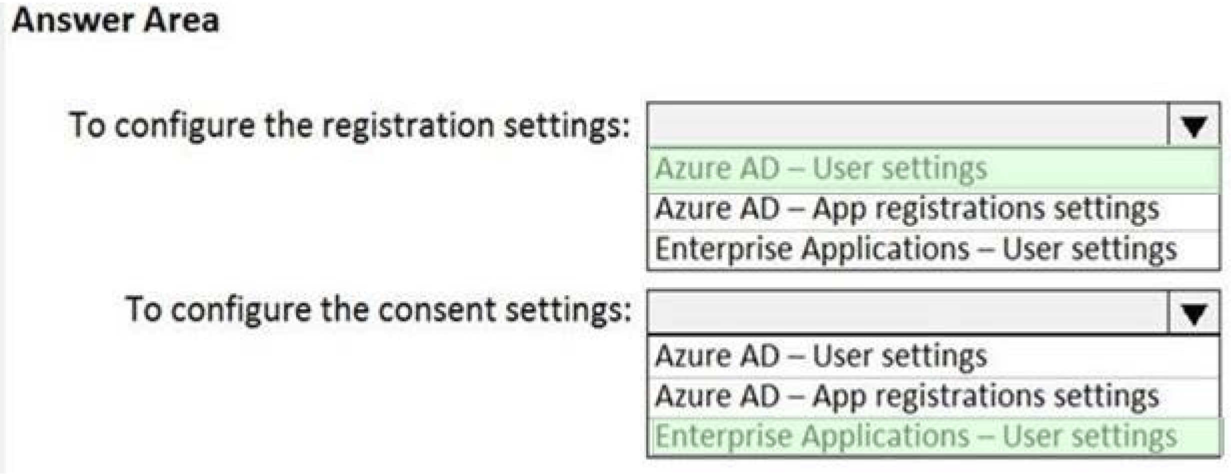


Answer Area

To configure the registration settings:
- Azure AD – User settings
- Azure AD – App registrations settings
- Enterprise Applications – User settings

To configure the consent settings:
- Azure AD – User settings
- Azure AD – App registrations settings
- Enterprise Applications – User settings

Answer Area:



Answer Area

To configure the registration settings:
- [✓ Azure AD – User settings]
- Azure AD – App registrations settings
- Enterprise Applications – User settings

To configure the consent settings:
- Azure AD – User settings
- Azure AD – App registrations settings
- [✓ Enterprise Applications – User settings]

Section:

Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/configure-user-consent

02 - Manage identity and access

Case Study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

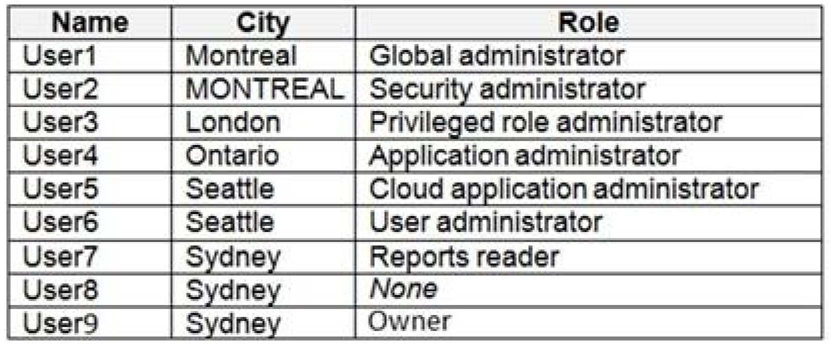
The company hosts its entire server infrastructure in Azure.

Contoso has two Azure subscriptions named Sub1 and Sub2. Both subscriptions are associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

Existing Environment

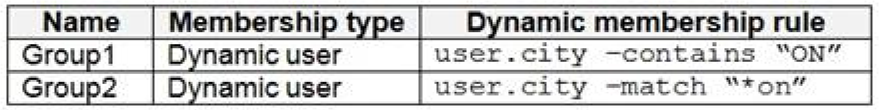
Azure AD

Contoso.com contains the users shown in the following table.



Name	City	Role
User1	Montreal	Global administrator
User2	MONTREAL	Security administrator
User3	London	Privileged role administrator
User4	Ontario	Application administrator
User5	Seattle	Cloud application administrator
User6	Seattle	User administrator
User7	Sydney	Reports reader
User8	Sydney	*None*
User9	Sydney	Owner

Contoso.com contains the security groups shown in the following table.

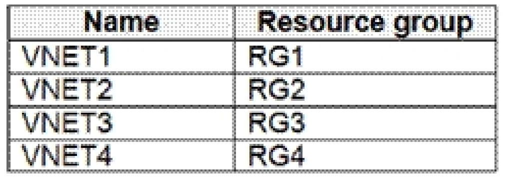


Name	Membership type	Dynamic membership rule
Group1	Dynamic user	`user.city -contains "ON"`
Group2	Dynamic user	`user.city -match "*on"`

Sub1

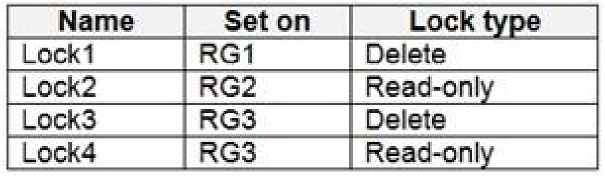
Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6.

User9 creates the virtual networks shown in the following table.



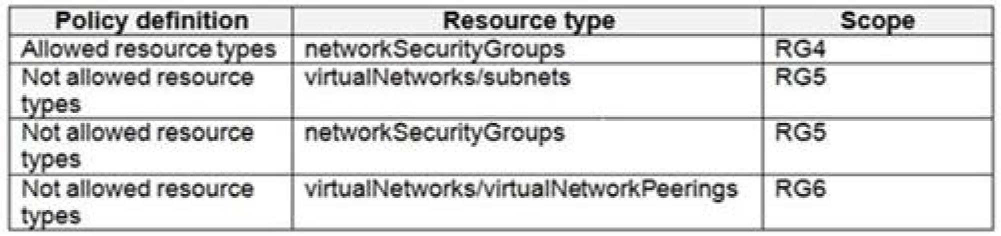
Name	Resource group
VNET1	RG1
VNET2	RG2
VNET3	RG3
VNET4	RG4

Sub1 contains the locks shown in the following table.



Name	Set on	Lock type
Lock1	RG1	Delete
Lock2	RG2	Read-only
Lock3	RG3	Delete
Lock4	RG3	Read-only

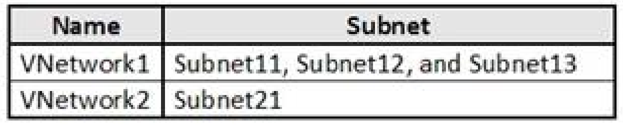
Sub1 contains the Azure policies shown in the following table.



Policy definition	Resource type	Scope
Allowed resource types	networkSecurityGroups	RG4
Not allowed resource types	virtualNetworks/subnets	RG5
Not allowed resource types	networkSecurityGroups	RG5
Not allowed resource types	virtualNetworks/virtualNetworkPeerings	RG6

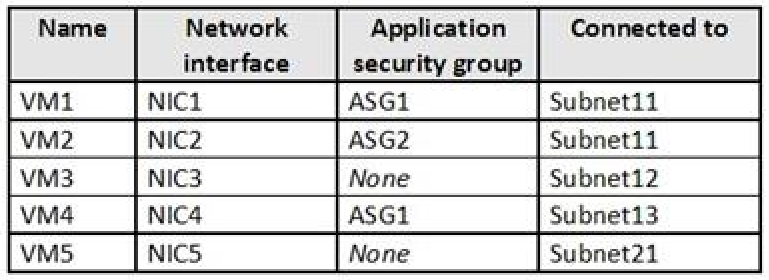
Sub2

Sub2 contains the virtual networks shown in the following table.



Name	Subnet
VNetwork1	Subnet11, Subnet12, and Subnet13
VNetwork2	Subnet21

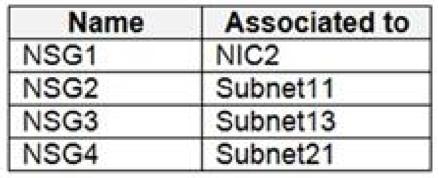
Sub2 contains the virtual machines shown in the following table.



Name	Network interface	Application security group	Connected to
VM1	NIC1	ASG1	Subnet11
VM2	NIC2	ASG2	Subnet11
VM3	NIC3	*None*	Subnet12
VM4	NIC4	ASG1	Subnet13
VM5	NIC5	*None*	Subnet21

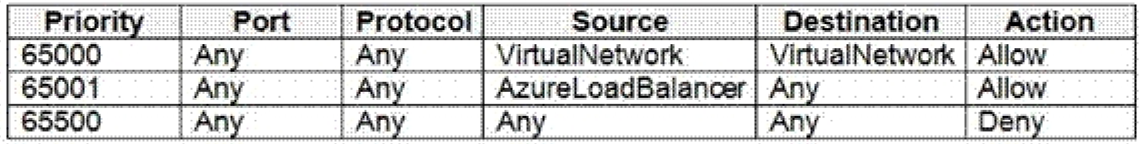
All virtual machines have public IP addresses and the Web Server (IIS) role installed. The firewalls for each virtual machine allow ping requests and web requests.

Sub2 contains the network security groups (NSGs) shown in the following table.



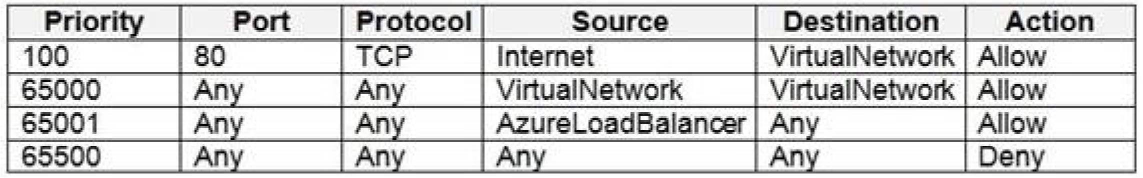
Name	Associated to
NSG1	NIC2
NSG2	Subnet11
NSG3	Subnet13
NSG4	Subnet21

NSG1 has the inbound security rules shown in the following table.



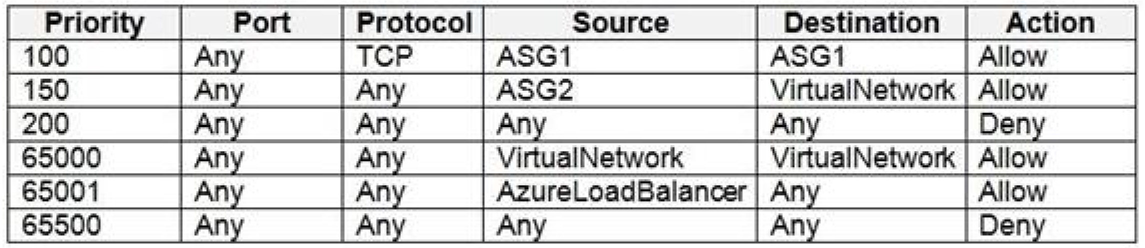
Priority	Port	Protocol	Source	Destination	Action
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG2 has the inbound security rules shown in the following table.



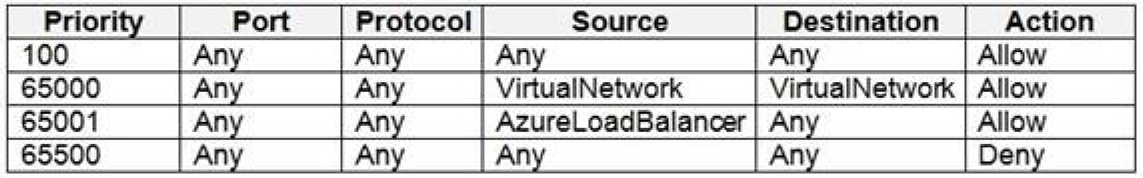
Priority	Port	Protocol	Source	Destination	Action
100	80	TCP	Internet	VirtualNetwork	Allow
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG3 has the inbound security rules shown in the following table.



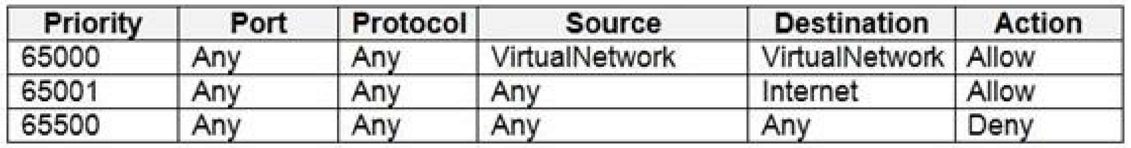
Priority	Port	Protocol	Source	Destination	Action
100	Any	TCP	ASG1	ASG1	Allow
150	Any	Any	ASG2	VirtualNetwork	Allow
200	Any	Any	Any	Any	Deny
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG4 has the inbound security rules shown in the following table.



Priority	Port	Protocol	Source	Destination	Action
100	Any	Any	Any	Any	Allow
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG1, NSG2, NSG3, and NSG4 have the outbound security rules shown in the following table.



Priority	Port	Protocol	Source	Destination	Action
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	Any	Internet	Allow
65500	Any	Any	Any	Any	Deny

Technical requirements

Contoso identifies the following technical requirements:

Deploy Azure Firewall to VNetwork1 in Sub2.

Register an application named App2 in contoso.com.

Whenever possible, use the principle of least privilege.
Enable Azure AD Privileged Identity Management (PIM) for contoso.com.

QUESTION 1

You need to ensure that User2 can implement PIM.
What should you do first?

A. Assign User2 the Global administrator role.

B. Configure authentication methods for contoso.com.

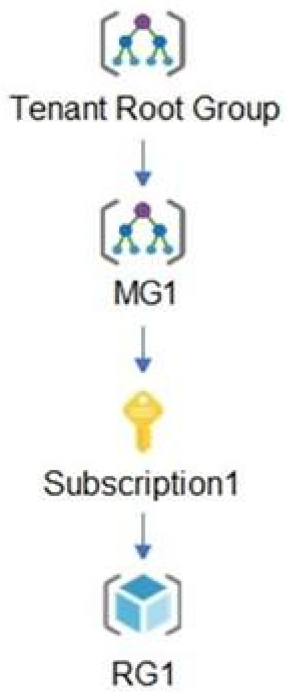
C. Configure the identity secure score for contoso.com.

D. Enable multi-factor authentication (MFA) for User2.

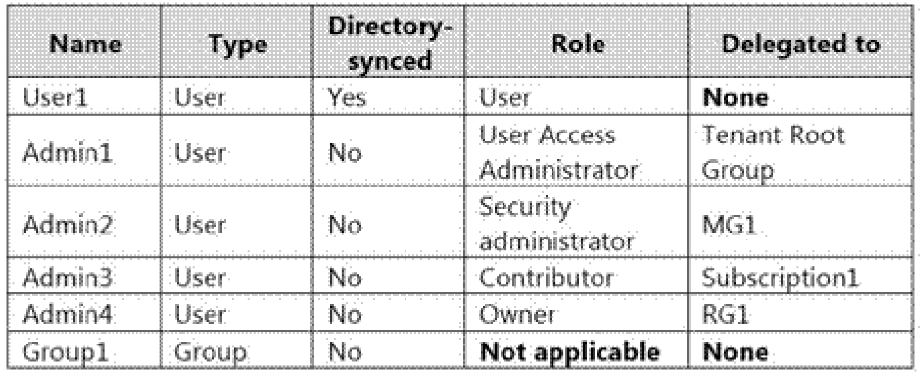
Correct Answer: A
Section:
Explanation:
To start using PIM in your directory, you must first enable PIM.
1. Sign in to the Azure portal as a Global Administrator of your directory.
You must be a Global Administrator with an organizational account (for example, @yourdomain.com), not a Microsoft account (for example, @outlook.com), to enable PIM for a directory. Scenario: Technical requirements include: Enable Azure AD Privileged Identity Management (PIM) for contoso.com
References:
https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-getting-started

03 - Manage identity and access

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.
To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.
At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.
To start the case study
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.
General Overview
Fabrikam, Inc. is a consulting company that has a main office in Montreal and branch offices in Seattle and New York. Fabrikam has IT, human resources (HR), and finance departments.
Existing Environment
Network Environment
Fabrikam has a Microsoft 365 subscription and an Azure subscription named subscription1.
The network contains an on-premises Active Directory domain named Fabrikam.com. The domain contains two organizational units (OUs) named OU1 and OU2. Azure AD Connect cloud sync syncs only OU1.
The Azure resources hierarchy is shown in the following exhibit.

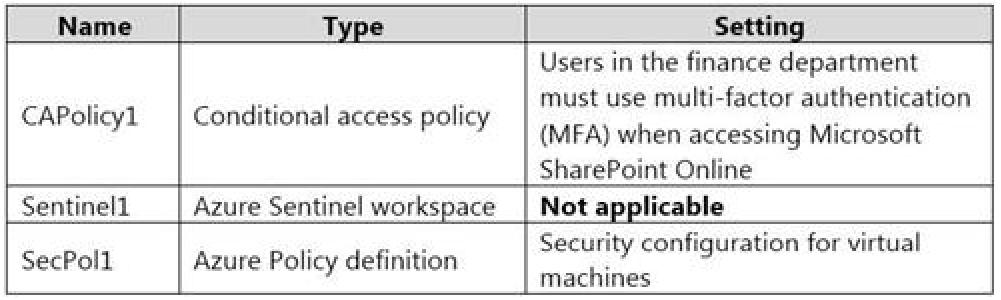


The Azure Active Directory (Azure AD) tenant contains the users shown in the following table.



Name	Type	Directory-synced	Role	Delegated to
User1	User	Yes	User	**None**
Admin1	User	No	User Access Administrator	Tenant Root Group
Admin2	User	No	Security administrator	MG1
Admin3	User	No	Contributor	Subscription1
Admin4	User	No	Owner	RG1
Group1	Group	No	**Not applicable**	**None**

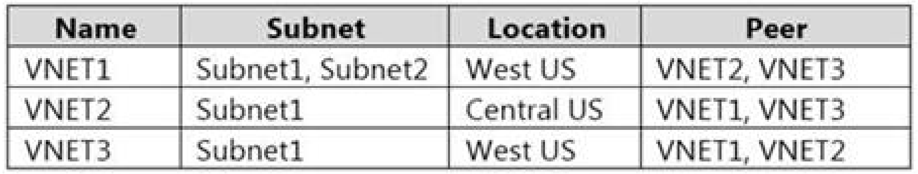
Azure AD contains the resources shown in the following table.



Name	Type	Setting
CAPolicy1	Conditional access policy	Users in the finance department must use multi-factor authentication (MFA) when accessing Microsoft SharePoint Online
Sentinel1	Azure Sentinel workspace	**Not applicable**
SecPol1	Azure Policy definition	Security configuration for virtual machines

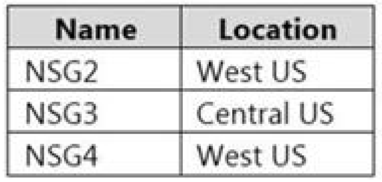
Subscription1 Resources

Subscription1 contains the virtual networks shown in the following table.



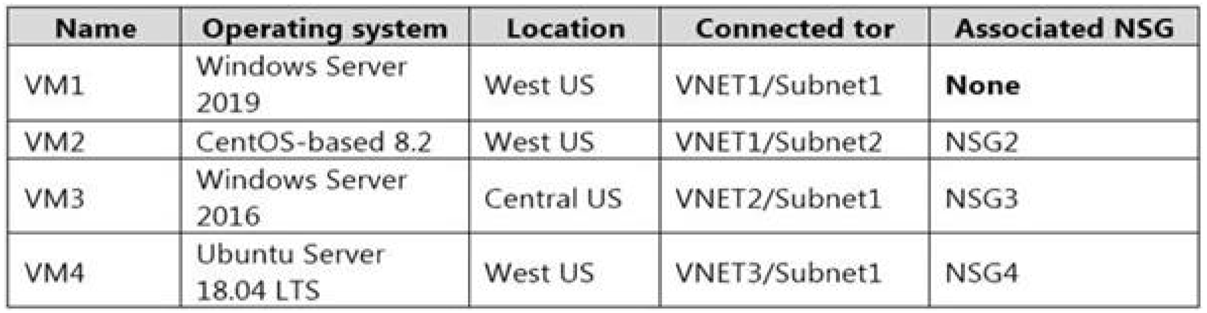
Name	Subnet	Location	Peer
VNET1	Subnet1, Subnet2	West US	VNET2, VNET3
VNET2	Subnet1	Central US	VNET1, VNET3
VNET3	Subnet1	West US	VNET1, VNET2

Subscription1 contains the network security groups (NSGs) shown in the following table.



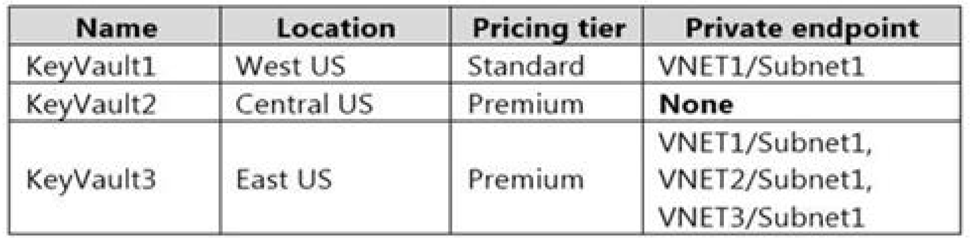
Name	Location
NSG2	West US
NSG3	Central US
NSG4	West US

Subscription1 contains the virtual machines shown in the following table.



Name	Operating system	Location	Connected tor	Associated NSG
VM1	Windows Server 2019	West US	VNET1/Subnet1	**None**
VM2	CentOS-based 8.2	West US	VNET1/Subnet2	NSG2
VM3	Windows Server 2016	Central US	VNET2/Subnet1	NSG3
VM4	Ubuntu Server 18.04 LTS	West US	VNET3/Subnet1	NSG4

Subscription1 contains the Azure key vaults shown in the following table.



Name	Location	Pricing tier	Private endpoint
KeyVault1	West US	Standard	VNET1/Subnet1
KeyVault2	Central US	Premium	**None**
KeyVault3	East US	Premium	VNET1/Subnet1, VNET2/Subnet1, VNET3/Subnet1

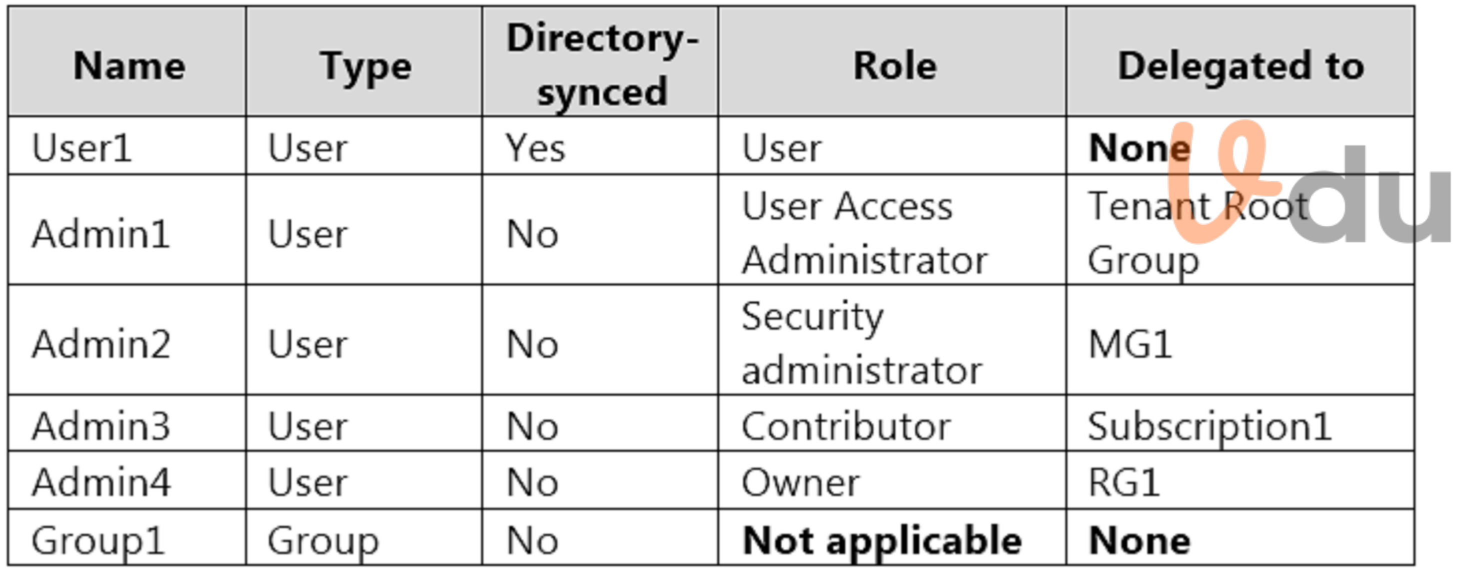
Subscription1 contains a storage account named storage1 in the West US Azure region.

Planned Changes and Requirements

Planned Changes

Fabrikam plans to implement the following changes:

Create two application security groups as shown in the following table.



Name	Type	Directory-synced	Role	Delegated to
User1	User	Yes	User	**None**
Admin1	User	No	User Access Administrator	Tenant Root Group
Admin2	User	No	Security administrator	MG1
Admin3	User	No	Contributor	Subscription1
Admin4	User	No	Owner	RG1
Group1	Group	No	**Not applicable**	**None**

Associate the network interface of VM1 to ASG1.

Deploy SecPol1 by using Azure Security Center.

Deploy a third-party app named App1. A version of App1 exists for all available operating systems.

Create a resource group named RG2.

Sync OU2 to Azure AD.

Add User1 to Group1.

Technical Requirements

Fabrikam identifies the following technical requirements:

The finance department users must reauthenticate after three hours when they access SharePoint Online. Storage1 must be encrypted by using customer-managed keys and automatic key rotation.

From Sentinel1, you must ensure that the following notebooks can be launched:

- Entity Explorer – Account
- Entity Explorer – Windows Host
- Guided Investigation Process Alerts

VM1, VM2, and VM3 must be encrypted by using Azure Disk Encryption.

Just in time (JIT) VM access for VM1, VM2, and VM3 must be enabled.

App1 must use a secure connection string stored in KeyVault1.

KeyVault1 traffic must NOT travel over the internet.

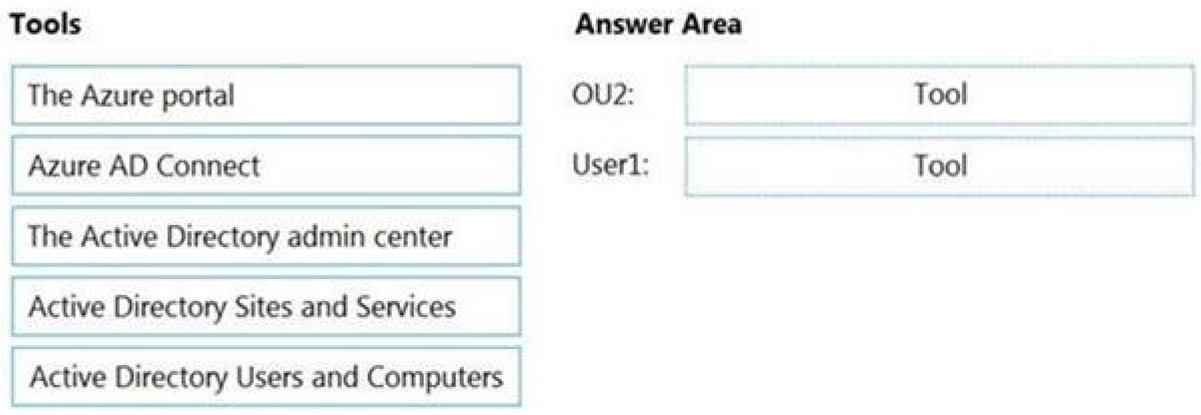
QUESTION 1

DRAG DROP

You need to perform the planned changes for OU2 and User1.

Which tools should you use? To answer, drag the appropriate tools to the correct resources. Each tool may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content. NOTE: Each correct selection is worth one point.

Select and Place:



Tools

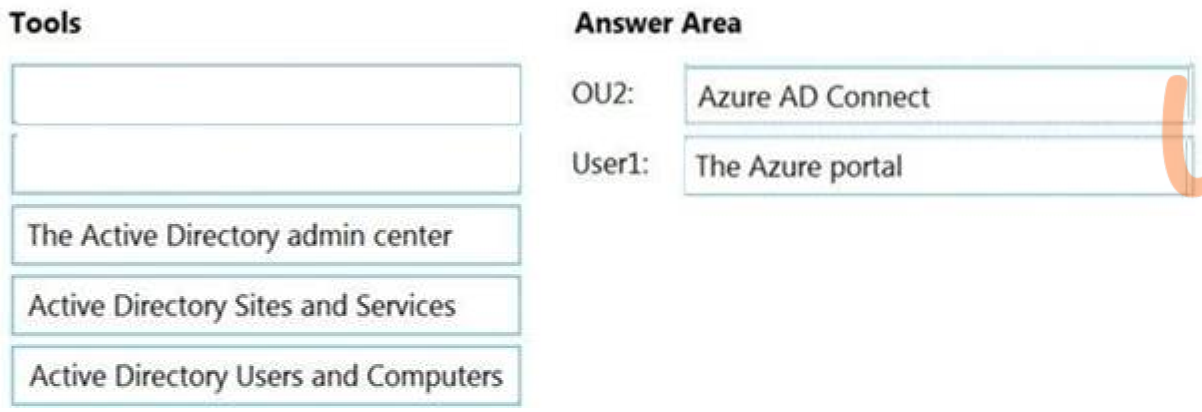
- The Azure portal
- Azure AD Connect
- The Active Directory admin center
- Active Directory Sites and Services
- Active Directory Users and Computers

Answer Area

OU2: Tool

User1: Tool

Correct Answer:



Tools

- The Active Directory admin center
- Active Directory Sites and Services
- Active Directory Users and Computers

Answer Area

OU2: Azure AD Connect

User1: The Azure portal

Section:

Explanation:

QUESTION 2

You need to meet the technical requirements for the finance department users.

Which CAPolicy1 settings should you modify?

A. Cloud apps or actions

B. Conditions

C. Grant

D. Session

Correct Answer: D

Section:

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-session-lifetime

QUESTION 3

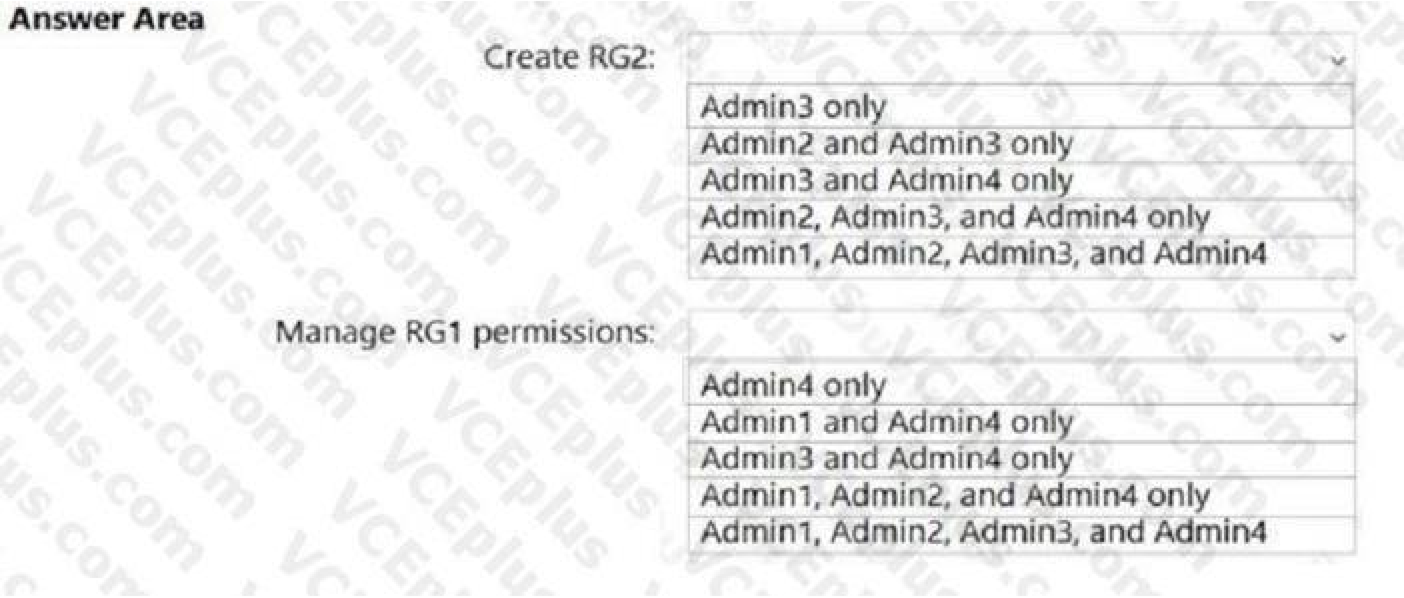
HOTSPOT

You need to delegate the creation of RG2 and the management of permissions for RG1.

Which users can perform each task? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

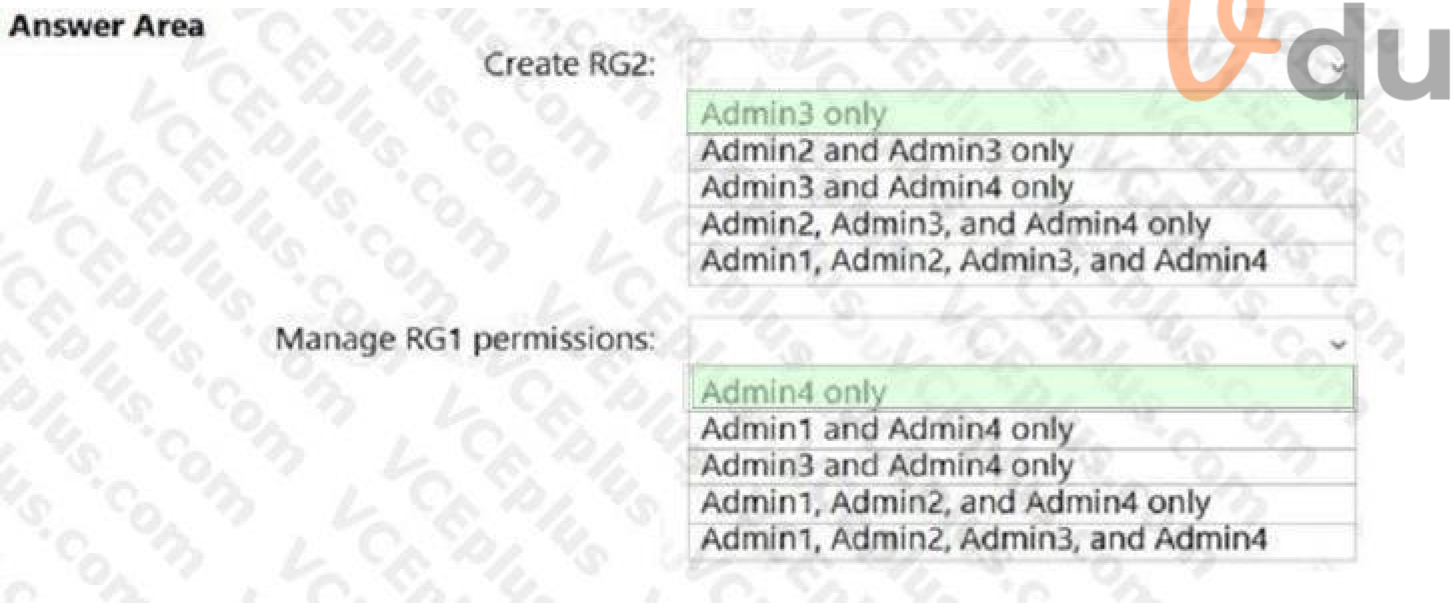
Create RG2:

- Admin3 only
- Admin2 and Admin3 only
- Admin3 and Admin4 only
- Admin2, Admin3, and Admin4 only
- Admin1, Admin2, Admin3, and Admin4

Manage RG1 permissions:

- Admin4 only
- Admin1 and Admin4 only
- Admin3 and Admin4 only
- Admin1, Admin2, and Admin4 only
- Admin1, Admin2, Admin3, and Admin4

Answer Area:



Answer Area

Create RG2:

- [✓ Admin3 only]
- Admin2 and Admin3 only
- Admin3 and Admin4 only
- Admin2, Admin3, and Admin4 only
- Admin1, Admin2, Admin3, and Admin4

Manage RG1 permissions:

- [✓ Admin4 only]
- Admin1 and Admin4 only
- Admin3 and Admin4 only
- Admin1, Admin2, and Admin4 only
- Admin1, Admin2, Admin3, and Admin4

Section:

Explanation:

Box 1: Admin3 only

The Contributor role has the necessary write permissions to create the resource group.

Box 2: Admin4 only

You need Owner level access to be able to manage permissions. The Contributor role can do most things but cannot modify permissions on existing objects.

04 - Manage identity and access

QUESTION 1

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a hybrid configuration of Azure Active Directory (Azure AD).
You have an Azure HDInsight cluster on a virtual network.
You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials.
You need to configure the environment to support the planned authentication.
Solution: You deploy an Azure AD Application Proxy.
Does this meet the goal?

A. Yes
B. No

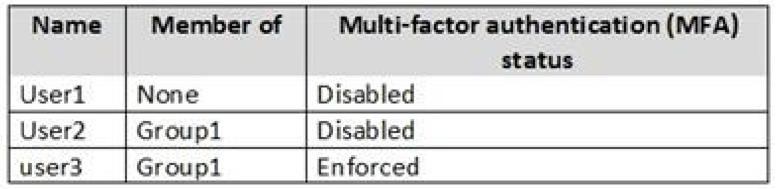
Correct Answer: B
Section:
Explanation:
Instead, you connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.
Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions:
Create Azure Virtual Network.
Create a custom DNS server in the Azure Virtual Network.
Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver. Configure forwarding between the custom DNS server and your on-premises DNS server.
Reference:
https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network

QUESTION 2
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure Subscription named Sub1.
You have an Azure Storage account named Sa1 in a resource group named RG1.
Users and applications access the blob service and the file service in Sa1 by using several shared access signatures (SASs) and stored access policies.
You discover that unauthorized users accessed both the file service and the blob service.
You need to revoke all access to Sa1.
Solution: You regenerate the Azure storage account access keys.
Does this meet the goal?

A. Yes
B. No

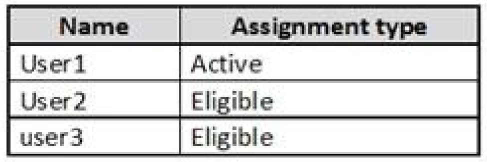
Correct Answer: A
Section:
Explanation:
Generating new storage account keys will invalidate all SAS's that were based on the previous keys.

QUESTION 3
HOTSPOT
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.



Name	Member of	Multi-factor authentication (MFA) status
User1	None	Disabled
User2	Group1	Disabled
user3	Group1	Enforced

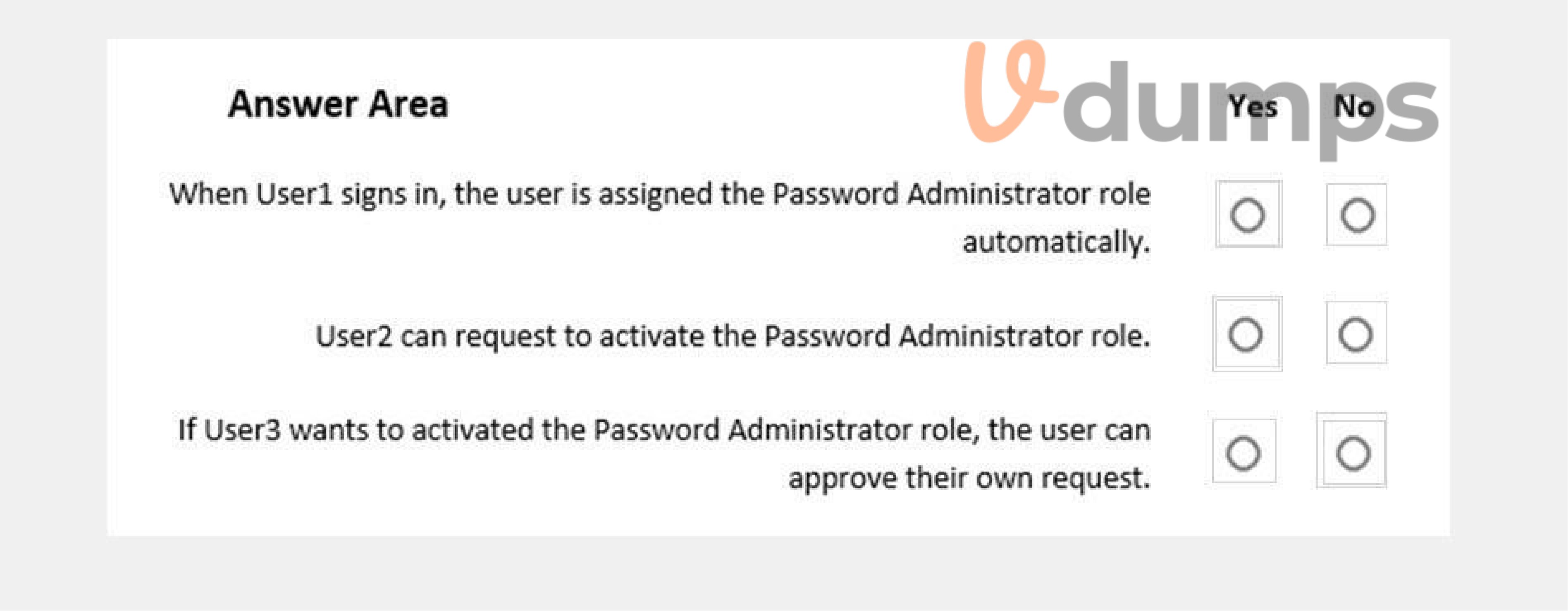
Azure AD Privileged Identity Management (PIM) is enabled for the tenant.
In PIM, the Password Administrator role has the following settings:
Maximum activation duration (hours): 2
Send email notifying admins of activation: Disable
Require incident/request ticket number during activation: Disable
Require Azure Multi-Factor Authentication for activation: Enable
Require approval to activate this role: Enable
Selected approver: Group1
You assign users the Password Administrator role as shown in the following table.



Name	Assignment type
User1	Active
User2	Eligible
user3	Eligible

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

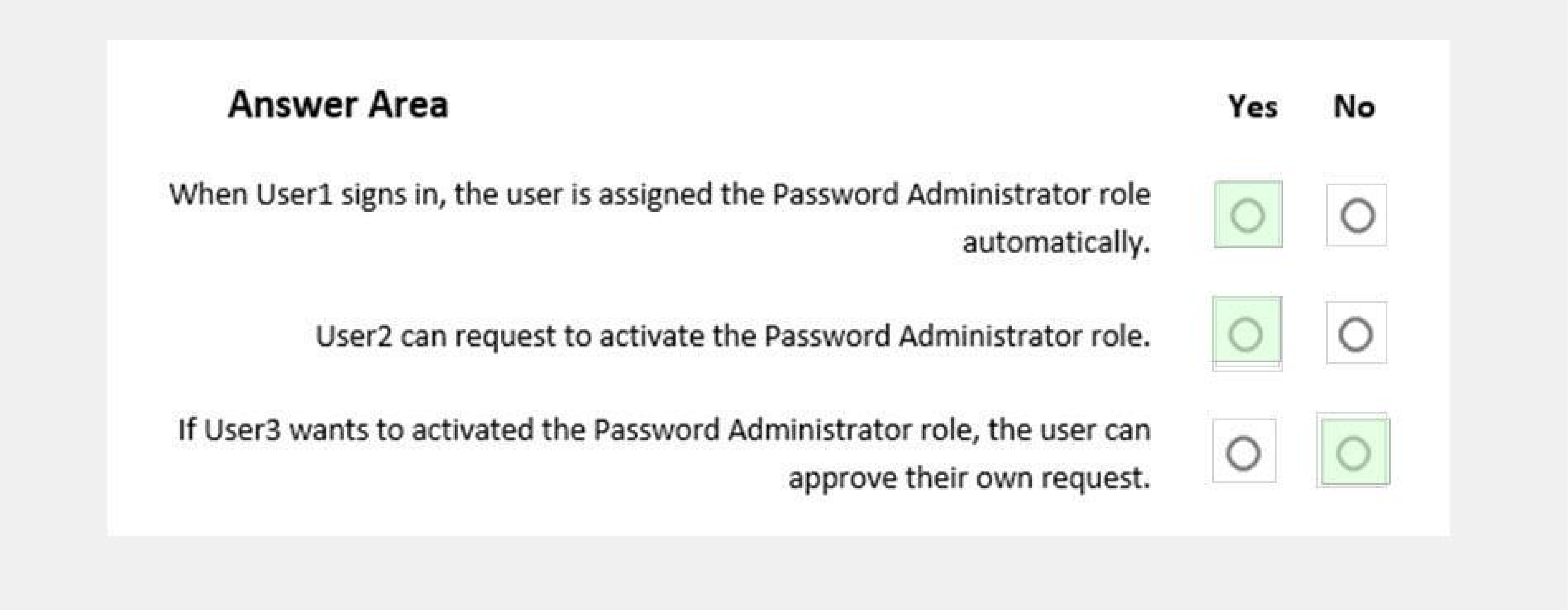
Hot Area:



Answer Area

	Yes	No
When User1 signs in, the user is assigned the Password Administrator role automatically.	○	○
User2 can request to activate the Password Administrator role.	○	○
If User3 wants to activated the Password Administrator role, the user can approve their own request.	○	○

Answer Area:



Answer Area

	Yes	No
When User1 signs in, the user is assigned the Password Administrator role automatically.	[✓ ○]	○
User2 can request to activate the Password Administrator role.	[✓ ○]	○
If User3 wants to activated the Password Administrator role, the user can approve their own request.	○	[✓ ○]

Section:
Explanation:
Box 1: Yes
Active assignments don't require the member to perform any action to use the role. Members assigned as active have the privileges assigned to the role at all times.
Box 2: Yes
While Multi-Factor Authentication is disabled for User2 and the setting Require Azure Multi-Factor Authentication for activation is enabled, User2 can request the role but will need to enable MFA to use the role.
Note: Eligible assignments require the member of the role to perform an action to use the role. Actions might include performing a multi-factor authentication (MFA) check, providing a business justification, or requesting approval from designated approvers.
Box 3: No
User3 is Group1, which is a Selected Approver Group, however, self-approval is not allowed and someone else from group is required to approve the request.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-resource-roles-assign-roles

QUESTION 4
You have a hybrid configuration of Azure Active Directory (Azure AD) that has Single Sign-On (SSO) enabled. You have an Azure SQL Database instance that is configured to support Azure AD authentication.
Database developers must connect to the database instance from the domain joined device and authenticate by using their on-premises Active Directory account.
You need to ensure that developers can connect to the instance by using Microsoft SQL Server Management Studio. The solution must minimize authentication prompts.
Which authentication method should you recommend?

A. Active Directory - Password
B. Active Directory - Universal with MFA support
C. SQL Server Authentication
D. Active Directory - Integrated

Correct Answer: D
Section:
Explanation:
Active Directory - Integrated
Azure Active Directory Authentication is a mechanism of connecting to Microsoft Azure SQL Database by using identities in Azure Active Directory (Azure AD). Use this method for connecting to SQL Database if you are logged in to Windows using your Azure Active Directory credentials from a federated domain.

Reference:
https://docs.microsoft.com/en-us/sql/ssms/f1-help/connect-to-server-database-engine?view=sql-server-2017 https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication-configure

QUESTION 5

You plan to use Azure Resource Manager templates to perform multiple deployments of identically configured Azure virtual machines. The password for the administrator account of each deployment is stored as a secret in different Azure key vaults.

You need to identify a method to dynamically construct a resource ID that will designate the key vault containing the appropriate secret during each deployment. The name of the key vault and the name of the secret will be provided as inline parameters.

What should you use to construct the resource ID?

A. a key vault access policy

B. a linked template

C. a parameters file

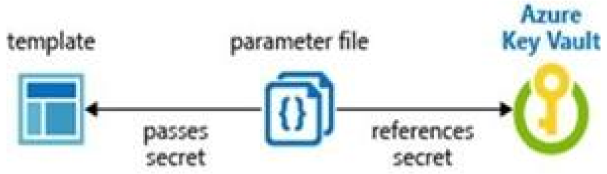
D. an automation account

Correct Answer: C

Section:

Explanation:

You reference the key vault in the parameter file, not the template. The following image shows how the parameter file references the secret and passes that value to the template.



Reference:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-keyvault-parameter

QUESTION 6

Note: This question-is part of a series of questions that present the same scenario. Each question-in the series contains a unique solution that might meet the stated goals. Some question-sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question-in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You have an Azure Subscription named Sub1.

You have an Azure Storage account named Sa1 in a resource group named RG1.

Users and applications access the blob service and the file service in Sa1 by using several shared access signatures (SASs) and stored access policies. You discover that unauthorized users accessed both the file service and the blob service.

You need to revoke all access to Sa1.

Solution: You create a new stored access policy.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Section:

Explanation:

Creating a new (additional) stored access policy with have no effect on the existing policy or the SAS's linked to it. To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier. Changing the signed identifier breaks the associations between any existing signatures and the stored access policy. Deleting or renaming the stored access policy immediately effects all of the shared access signatures associated with it. References: https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy

QUESTION 7

Note: This question-is part of a series of questions that present the same scenario. Each question-in the series contains a unique solution that might meet the stated goals. Some question-sets might have more than one

correct solution, while others might not have a correct solution.
After you answer a question-in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You have a hybrid configuration of Azure Active Directory (AzureAD).
You have an Azure HDInsight cluster on a virtual network.
You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials. You need to configure the environment to support the planned authentication.
Solution: You deploy the On-premises data gateway to the on-premises network.
Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section:
Explanation:
Instead, you connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway. Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions: Create Azure Virtual Network. Create a custom DNS server in the Azure Virtual Network.
Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver. Configure forwarding between the custom DNS server and your on-premises DNS server. References:
https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network

QUESTION 8
Note: This question-is part of a series of questions that present the same scenario. Each question-in the series contains a unique solution that might meet the stated goals. Some question-sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question-in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You have a hybrid configuration of Azure Active Directory (AzureAD).
You have an Azure HDInsight cluster on a virtual network.
You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials. You need to configure the environment to support the planned authentication.
Solution: You create a site-to-site VPN between the virtual network and the on-premises network.
Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section:
Explanation:
You can connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway. Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions: Create Azure Virtual Network. Create a custom DNS server in the Azure Virtual Network.
Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver. Configure forwarding between the custom DNS server and your on-premises DNS server. References:
https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network

QUESTION 9
Your network contains an Active Directory forest named contoso.com. The forest contains a single domain. You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com. You plan to deploy Azure AD Connect and to integrate Active Directory and the Azure AD tenant.
You need to recommend an integration solution that meets the following requirements:
Ensures that password policies and user logon restrictions apply to user accounts that are synced to the tenant Minimizes the number of servers required for the solution. Which authentication method should you include in the recommendation?

A. federated identity with Active Directory Federation Services (AD FS)
B. password hash synchronization with seamless single sign-on (SSO)
C. pass-through authentication with seamless single sign-on (SSO)

Correct Answer: B
Section:
Explanation:
Password hash synchronization requires the least effort regarding deployment, maintenance, and infrastructure. This level of effort typically applies to organizations that only need their users to sign in to Office 365, SaaS apps, and other Azure AD-based resources. When turned on, password hash synchronization is part of the Azure AD Connect sync process and runs every two minutes. Incorrect Answers:
A: A federated authentication system relies on an external trusted system to authenticate users. Some companies want to reuse their existing federated system investment with their Azure AD hybrid identity solution. The maintenance and management of the federated system falls outside the control of Azure AD. It's up to the organization by using the federated system to make sure it's deployed securely and can handle the authentication load. C: For pass-through authentication, you need one or more (we recommend three) lightweight agents installed on existing servers. These agents must have access to your on-premises Active Directory Domain Services, including your onpremises AD domain controllers. They need outbound access to the Internet and access to your domain controllers. For this reason, it's not supported to deploy the agents in a perimeter network. Pass-through Authentication requires unconstrained network access to domain controllers. All network traffic is encrypted and limited to authentication requests. References: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta

QUESTION 10
Your network contains an on-premises Active Directory domain named corp.contoso.com.
You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com. You sync all on-premises identities to Azure AD.
You need to prevent users who have a givenName attribute that starts with TEST from being synced to Azure AD. The solution must minimize administrative effort. What should you use?

A. Synchronization Rules Editor
B. Web Service Configuration Tool
C. the Azure AD Connect wizard
D. Active Directory Users and Computers

Correct Answer: A
Section:
Explanation:
Use the Synchronization Rules Editor and write attribute-based filtering rule.
References: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-the-configuration

QUESTION 11
Your company plans to create separate subscriptions for each department. Each subscription will be associated to the same Azure Active Directory (Azure AD) tenant.
You need to configure each subscription to have the same role assignments.
What should you use?

A. Azure Security Center
B. Azure Policy
C. Azure AD Privileged Identity Management (PIM)
D. Azure Blueprints

Correct Answer: D
Section:
Explanation:
Just as a blueprint allows an engineer or an architect to sketch a project's design parameters, Azure Blueprints enables cloud architects and central information technology groups to define a repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements.
Blueprints are a declarative way to orchestrate the deployment of various resource templates and other artifacts such as:
Role Assignments
Policy Assignments
Azure Resource Manager templates
Resource Groups
Reference:

https://docs.microsoft.com/en-us/azure/governance/blueprints/overview

QUESTION 12

You have an Azure subscription.
You create an Azure web app named Contoso1812 that uses an S1 App Service plan.
You plan to create a CNAME DNS record for www.contoso.com that points to Contoso1812.
You need to ensure that users can access Contoso1812 by using the https://www.contoso.com URL.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Turn on the system-assigned managed identity for Contoso1812.
B. Add a hostname to Contoso1812.
C. Scale out the App Service plan of Contoso1812.
D. Add a deployment slot to Contoso1812.
E. Scale up the App Service plan of Contoso1812.
F. Upload a PFX file to Contoso1812.

Correct Answer: B, F
Section:
Explanation:
B: You can configure Azure DNS to host a custom domain for your web apps. For example, you can create an Azure web app and have your users access it using either www.contoso.com or contoso.com as a fully qualified domain name (FQDN).
To do this, you have to create three records:
A root "A" record pointing to contoso.com
A root "TXT" record for verification
A "CNAME" record for the www name that points to the A record
F: To use HTTPS, you need to upload a PFX file to the Azure Web App. The PFX file will contain the SSL certificate required for HTTPS.
References:
https://docs.microsoft.com/en-us/azure/dns/dns-web-sites-custom-domain

QUESTION 13

Note: This question-is part of a series of questions that present the same scenario. Each question-in the series contains a unique solution that might meet the stated goals. Some question-sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question-in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You have an Azure subscription named Sub1.
You have an Azure Storage account named Sa1 in a resource group named RG1.
Users and applications access the blob service and the file service in Sa1 by using several shared access signatures (SASs) and stored access policies. You discover that unauthorized users accessed both the file service and the blob service.
You need to revoke all access to Sa1.
Solution: You create a lock on Sa1.
Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section:
Explanation:
To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier. Changing the signed identifier breaks the associations between any existing signatures and the stored access policy. Deleting or renaming the stored access policy immediately affects all of the shared access signatures associated with it. References:
https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy

QUESTION 14

DRAG DROP

You are implementing conditional access policies.

You must evaluate the existing Azure Active Directory (Azure AD) risk events and risk levels to configure and implement the policies.

You need to identify the risk level of the following risk events:

Users with leaked credentials

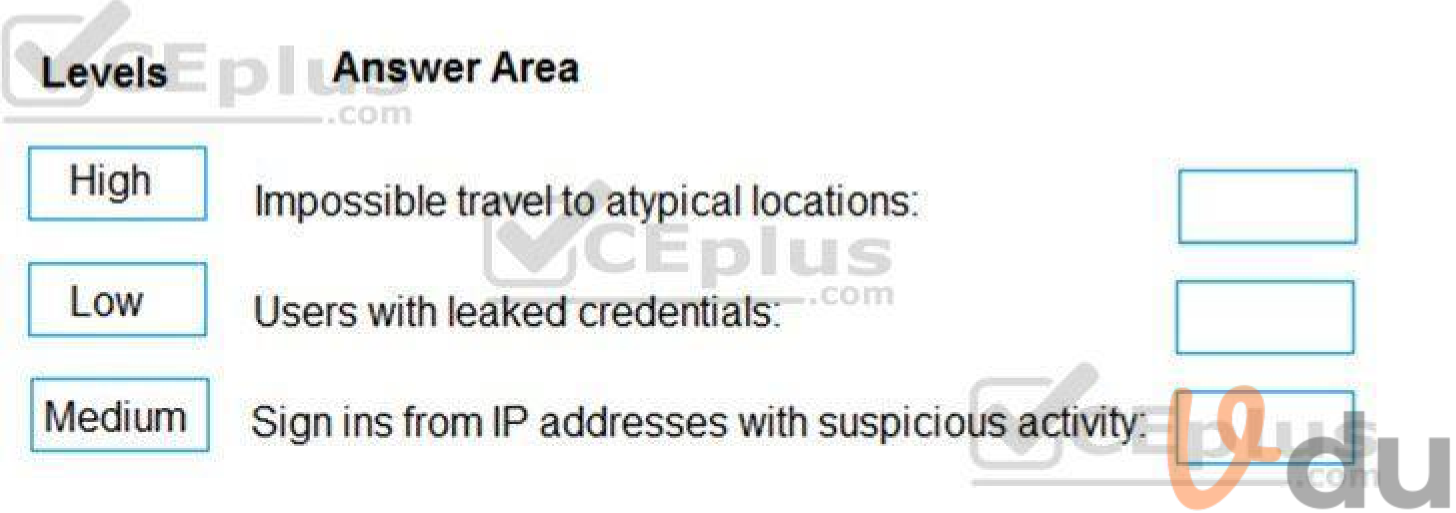
Impossible travel to atypical locations

Sign ins from IP addresses with suspicious activity

Which level should you identify for each risk event? To answer, drag the appropriate levels to the correct risk events. Each level may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Levels

High

Low

Medium

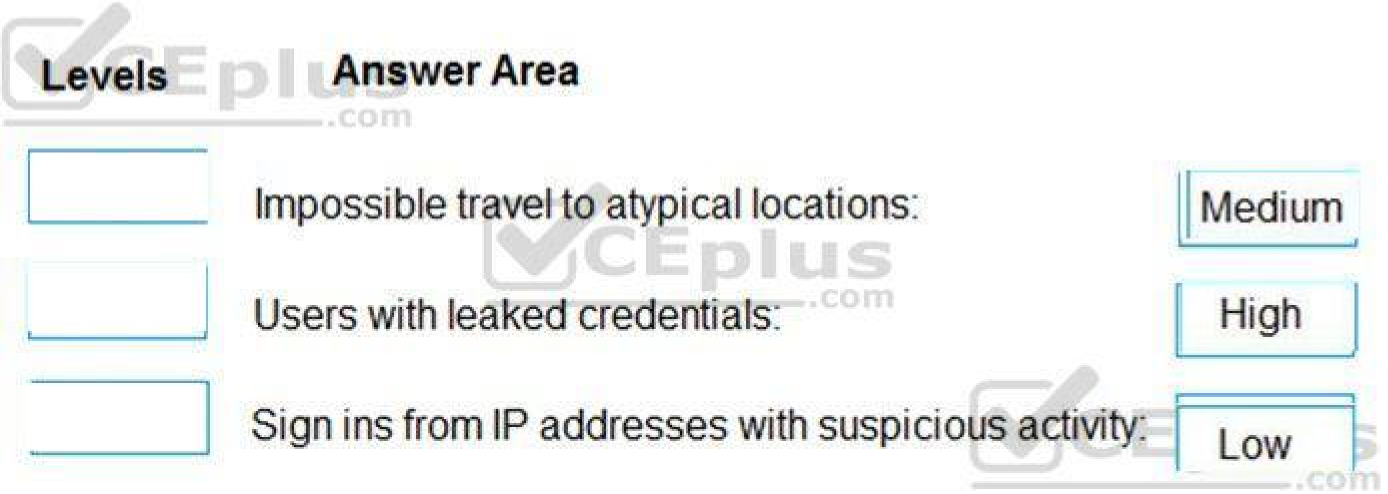
Answer Area

Impossible travel to atypical locations:

Users with leaked credentials:

Sign ins from IP addresses with suspicious activity:

Correct Answer:



Levels

Answer Area

Impossible travel to atypical locations: Medium

Users with leaked credentials: High

Sign ins from IP addresses with suspicious activity: Low

Section:

Explanation:

Azure AD Identity protection can detect six types of suspicious sign-in activities:

Users with leaked credentials

Sign-ins from anonymous IP addresses

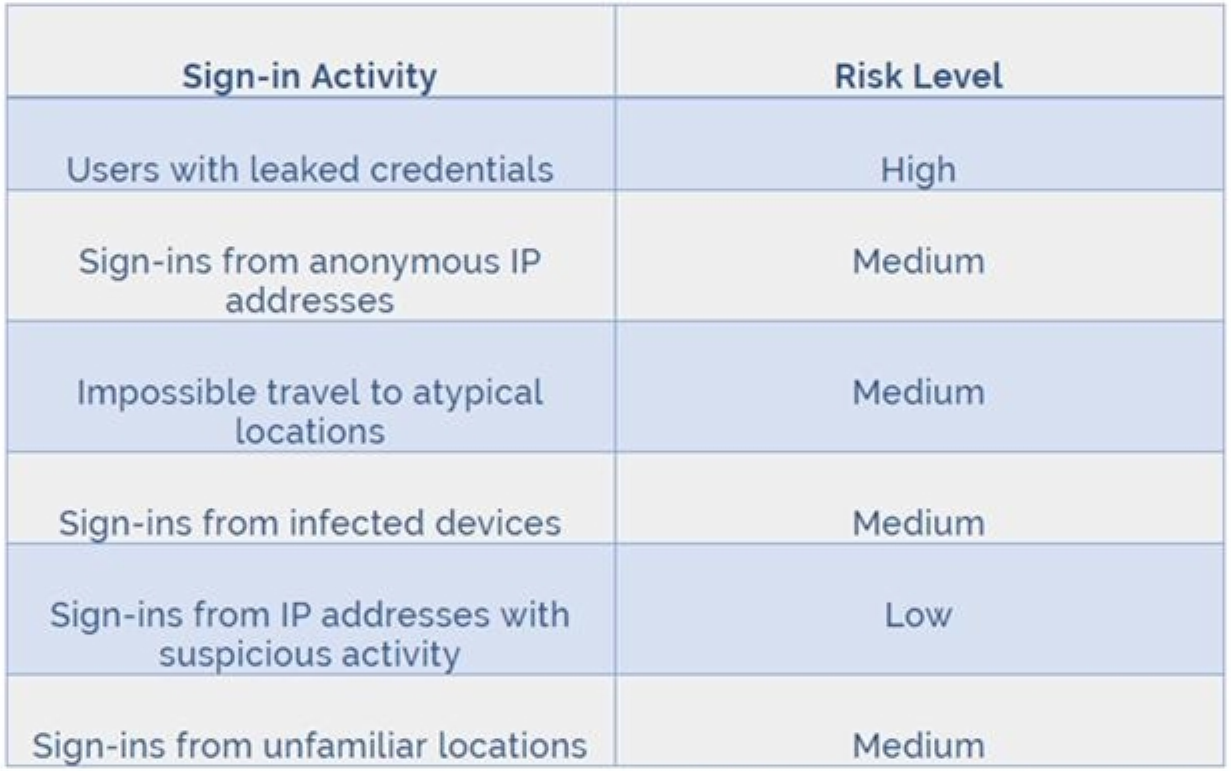
Impossible travel to atypical locations

Sign-ins from infected devices

Sign-ins from IP addresses with suspicious activity

Sign-ins from unfamiliar locations

These six types of events are categorized in to 3 levels of risks – High, Medium & Low:



Sign-in Activity	Risk Level
Users with leaked credentials	High
Sign-ins from anonymous IP addresses	Medium
Impossible travel to atypical locations	Medium
Sign-ins from infected devices	Medium
Sign-ins from IP addresses with suspicious activity	Low
Sign-ins from unfamiliar locations	Medium

References:
http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/

QUESTION 15
You have an Azure subscription.
You configure the subscription to use a different Azure Active Directory (Azure AD) tenant.
What are two possible effects of the change? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Role assignments at the subscription level are lost.
B. Virtual machine managed identities are lost.
C. Virtual machine disk snapshots are lost.
D. Existing Azure resources are deleted.

Correct Answer: A, B
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-how-subscriptions-associated-directory

QUESTION 16
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure Subscription named Sub1.
You have an Azure Storage account named Sa1 in a resource group named RG1.
Users and applications access the blob service and the file service in Sa1 by using several shared access signatures (SASs) and stored access policies.
You discover that unauthorized users accessed both the file service and the blob service.
You need to revoke all access to Sa1.
Solution: You generate new SASs.

Does this meet the goal?

A. Yes
B. No

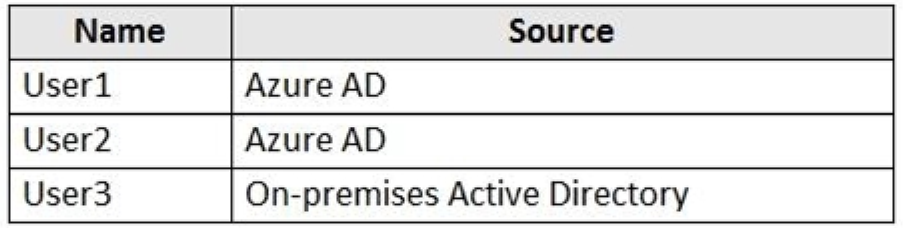
Correct Answer: B
Section:
Explanation:
Instead you should create a new stored access policy.
To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier. Changing the signed identifier breaks the associations between any existing signatures and the stored access policy.
Deleting or renaming the stored access policy immediately affects all of the shared access signatures associated with it.
References:
https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy

QUESTION 17
You have an Azure subscription that contains virtual machines.
You enable just in time (JIT) VM access to all the virtual machines.
You need to connect to a virtual machine by using Remote Desktop.
What should you do first?

A. From Azure Directory (Azure AD) Privileged Identity Management (PIM), activate the Security administrator user role.
B. From Azure Active Directory (Azure AD) Privileged Identity Management (PIM), activate the Owner role for the virtual machine.
C. From the Azure portal, select the virtual machine, select Connect, and then select Request access.
D. From the Azure portal, select the virtual machine and add the Network Watcher Agent virtual machine extension.

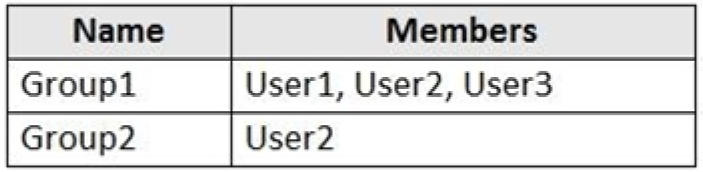
Correct Answer: C
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/connect-logon

QUESTION 18
HOTSPOT
Your network contains an on-premises Active Directory domain that syncs to an Azure Active Directory (Azure AD) tenant. The tenant contains the users shown in the following table.



Name	Source
User1	Azure AD
User2	Azure AD
User3	On-premises Active Directory

The tenant contains the groups shown in the following table.

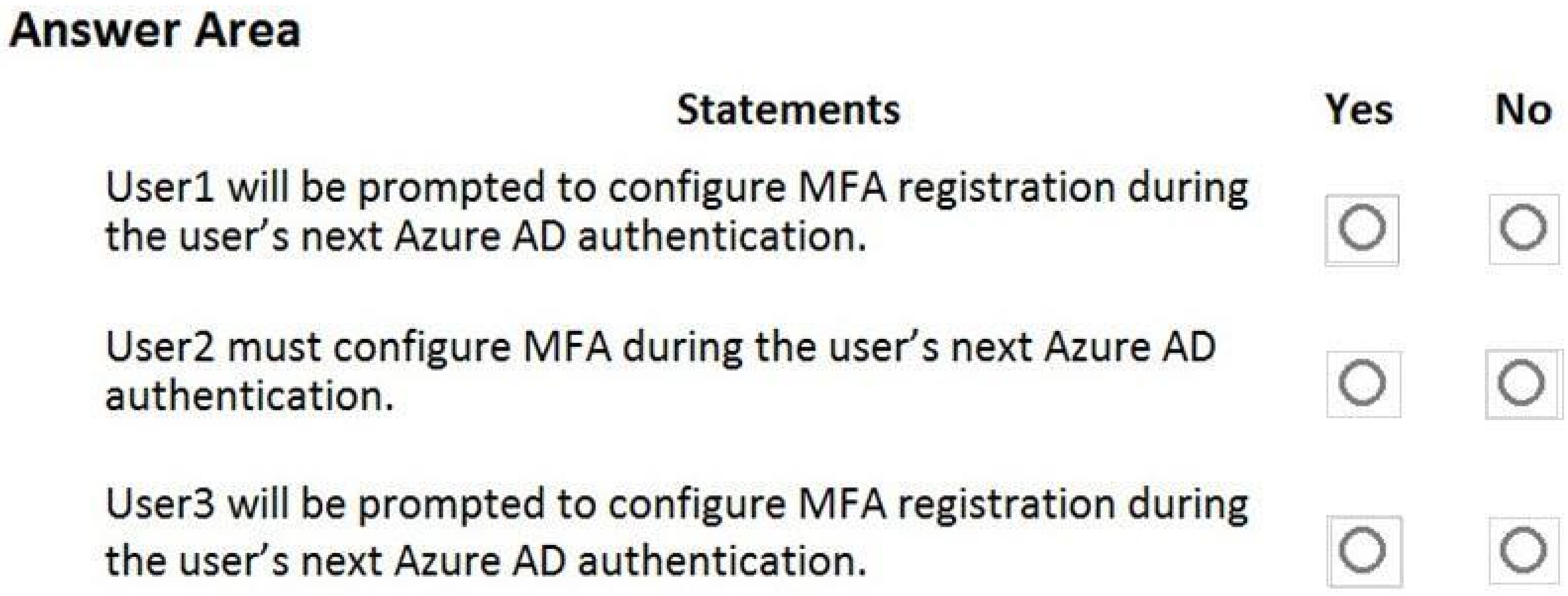


Name	Members
Group1	User1, User2, User3
Group2	User2

You configure a multi-factor authentication (MFA) registration policy that has the following settings:
Assignments:
- Include: Group1
- Exclude Group2

Controls: Require Azure MFA registration
Enforce Policy: On
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

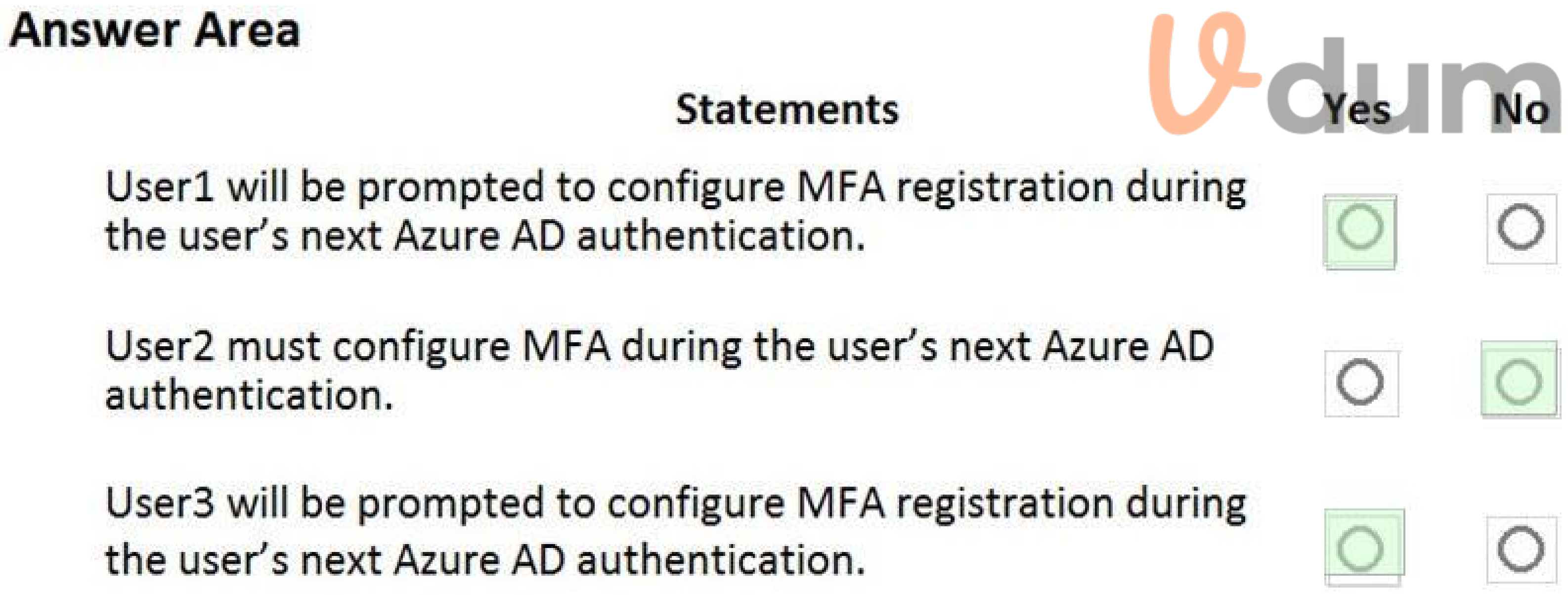
Hot Area:



Answer Area

Statements	Yes	No
User1 will be prompted to configure MFA registration during the user's next Azure AD authentication.	○	○
User2 must configure MFA during the user's next Azure AD authentication.	○	○
User3 will be prompted to configure MFA registration during the user's next Azure AD authentication.	○	○

Answer Area:



Answer Area

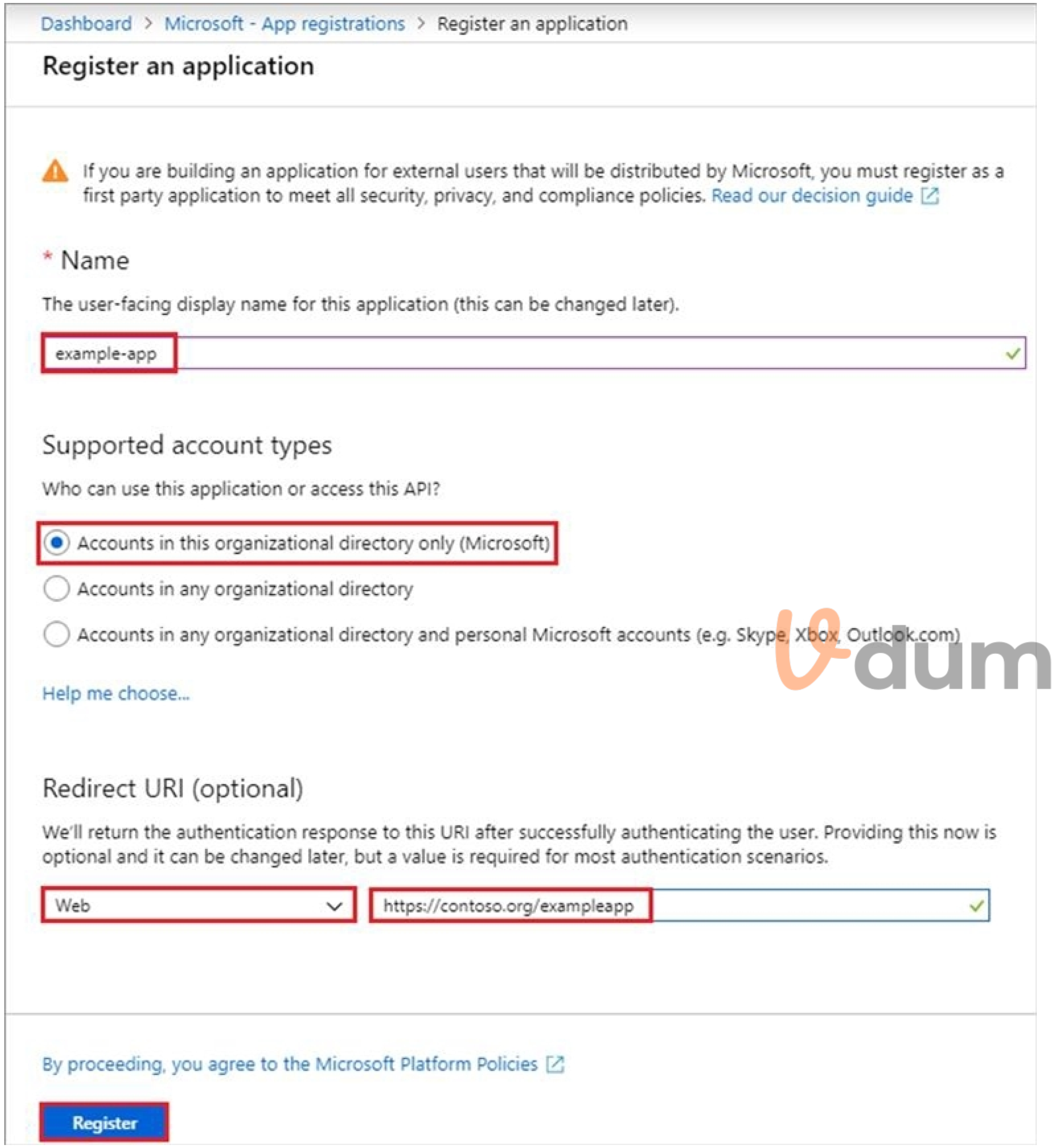
Statements	Yes	No
User1 will be prompted to configure MFA registration during the user's next Azure AD authentication.	●	○
User2 must configure MFA during the user's next Azure AD authentication.	○	●
User3 will be prompted to configure MFA registration during the user's next Azure AD authentication.	●	○

Section:
Explanation:

QUESTION 19
SIMULATION
The developers at your company plan to publish an app named App11641655 to Azure.
You need to ensure that the app is registered to Azure Active Directory (Azure AD). The registration must use the sign-on URLs of https://app.contoso.com.
To complete this task, sign in to the Azure portal and modify the Azure resources.

A.

Correct Answer: A
Section:
Explanation:
Answer: A
Explanation:
Step 1: Register the Application
1. Sign in to your Azure Account through the Azure portal.
2. Select Azure Active Directory.
3. Select App registrations.
4. Select New registration.
5. Name the application App11641655. Select a supported account type, which determines who can use the application. Under Redirect URI, select Web for the type of application you want to create. Enter the URI: https://app.contoso.com , where the access token is sent to.



Dashboard > Microsoft - App registrations > Register an application

Register an application

If you are building an application for external users that will be distributed by Microsoft, you must register as a first party application to meet all security, privacy, and compliance policies. Read our decision guide

* Name

The user-facing display name for this application (this can be changed later).

example-app

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Microsoft)

○ Accounts in any organizational directory

○ Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web | https://contoso.org/exampleapp

By proceeding, you agree to the Microsoft Platform Policies

6. Click Register

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal

QUESTION 20

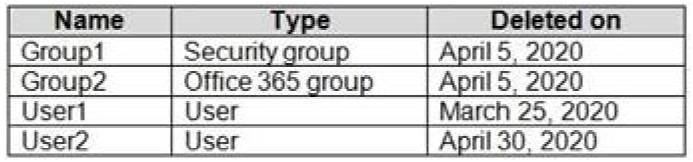
You have an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.

The User administrator role is assigned to a user named Admin1.
An external partner has a Microsoft account that uses the user1@outlook.com sign in.
Admin1 attempts to invite the external partner to sign in to the Azure AD tenant and receives the following error message: “Unable to invite user user1@outlook.com Generic authorization exception.”
You need to ensure that Admin1 can invite the external partner to sign in to the Azure AD tenant.
What should you do?

A. From the Roles and administrators blade, assign the Security administrator role to Admin1.
B. From the Organizational relationships blade, add an identity provider.
C. From the Custom domain names blade, add a custom domain.
D. From the Users blade, modify the External collaboration settings.

Correct Answer: D
Section:

QUESTION 21
You have an Azure Active Directory (Azure AD) tenant.
You have the deleted objects shown in the following table.



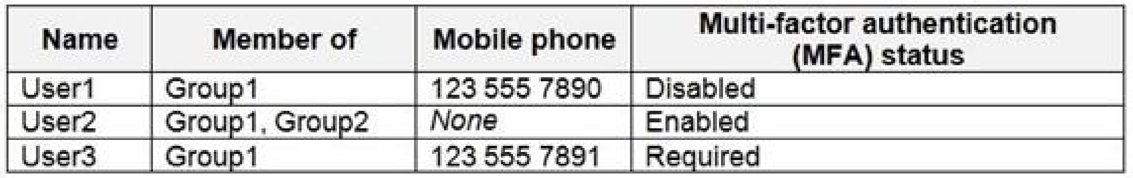
Name	Type	Deleted on
Group1	Security group	April 5, 2020
Group2	Office 365 group	April 5, 2020
User1	User	March 25, 2020
User2	User	April 30, 2020

On May 4, 2020, you attempt to restore the deleted objects by using the Azure Active Directory admin center.
Which two objects can you restore? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Group1
B. Group2
C. User2
D. User1

Correct Answer: B, C
Section:
Explanation:
Deleted users and deleted Office 365 groups are available for restore for 30 days.
You cannot restore a deleted security group.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-restore-deleted

QUESTION 22
HOTSPOT
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

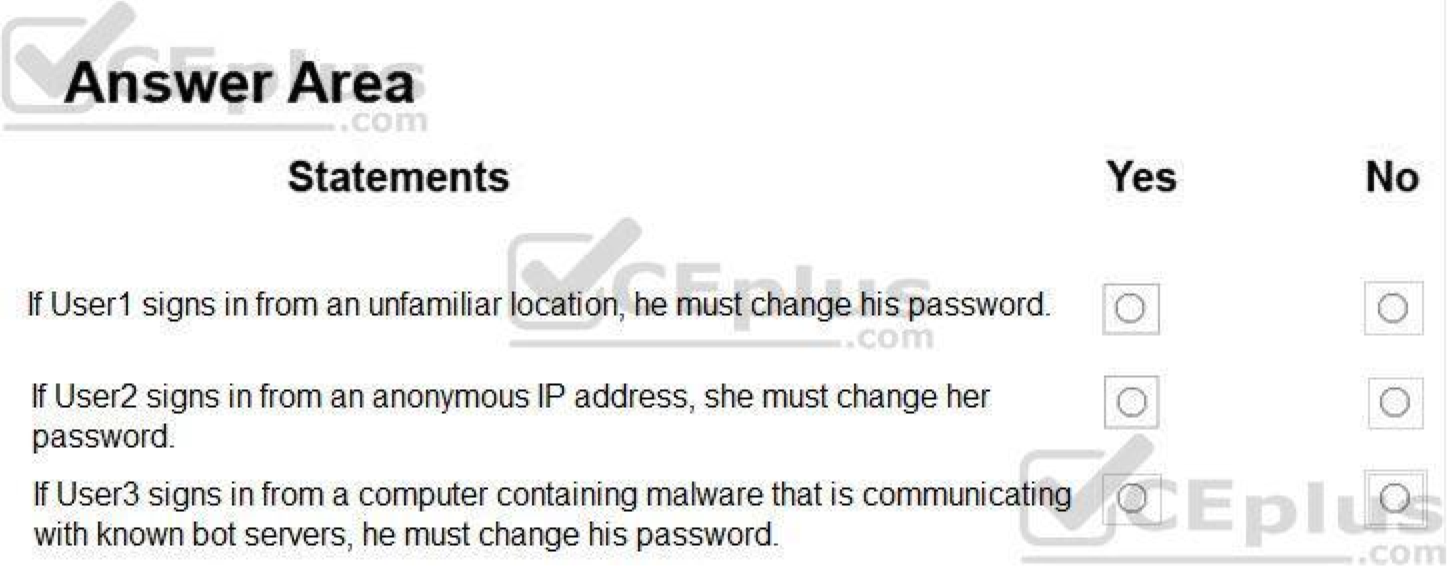


Name	Member of	Mobile phone	Multi-factor authentication (MFA) status
User1	Group1	123 555 7890	Disabled
User2	Group1, Group2	*None*	Enabled
User3	Group1	123 555 7891	Required

You create and enforce an Azure AD Identity Protection user risk policy that has the following settings:
Assignment: Include Group1, Exclude Group2
Conditions: Sign-in risk of Medium and above
Access: Allow access, Require password change

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

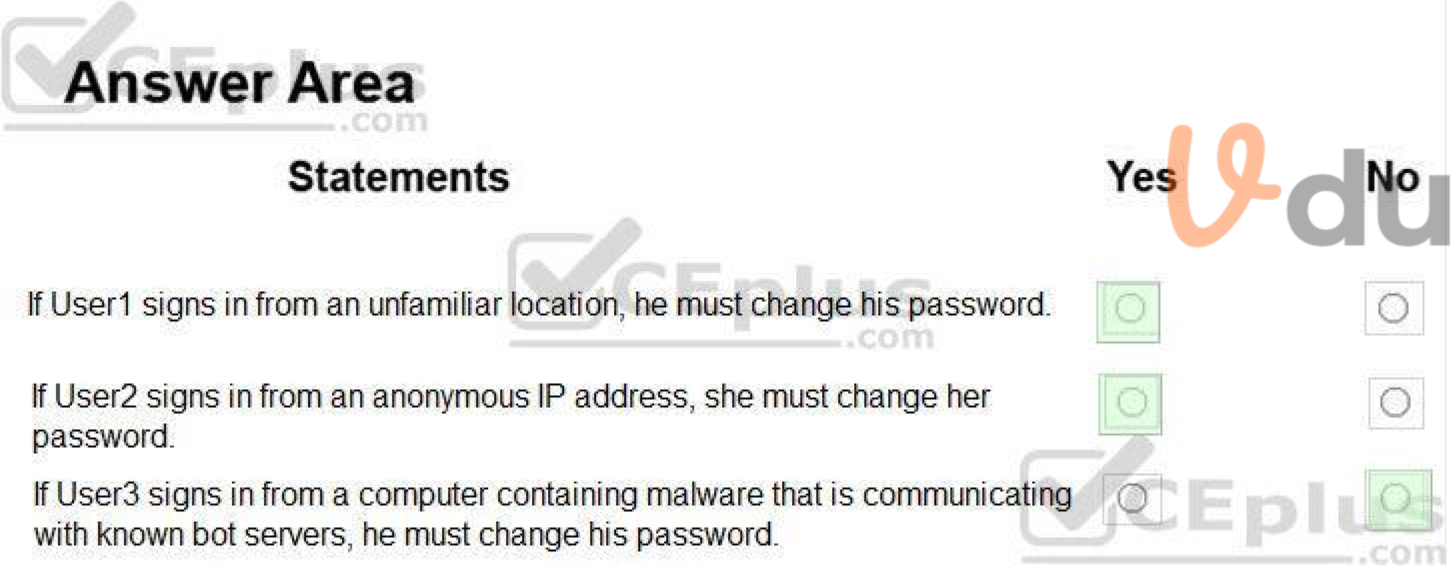
Hot Area:



Answer Area

Statements	Yes	No
If User1 signs in from an unfamiliar location, he must change his password.	○	○
If User2 signs in from an anonymous IP address, she must change her password.	○	○
If User3 signs in from a computer containing malware that is communicating with known bot servers, he must change his password.	○	○

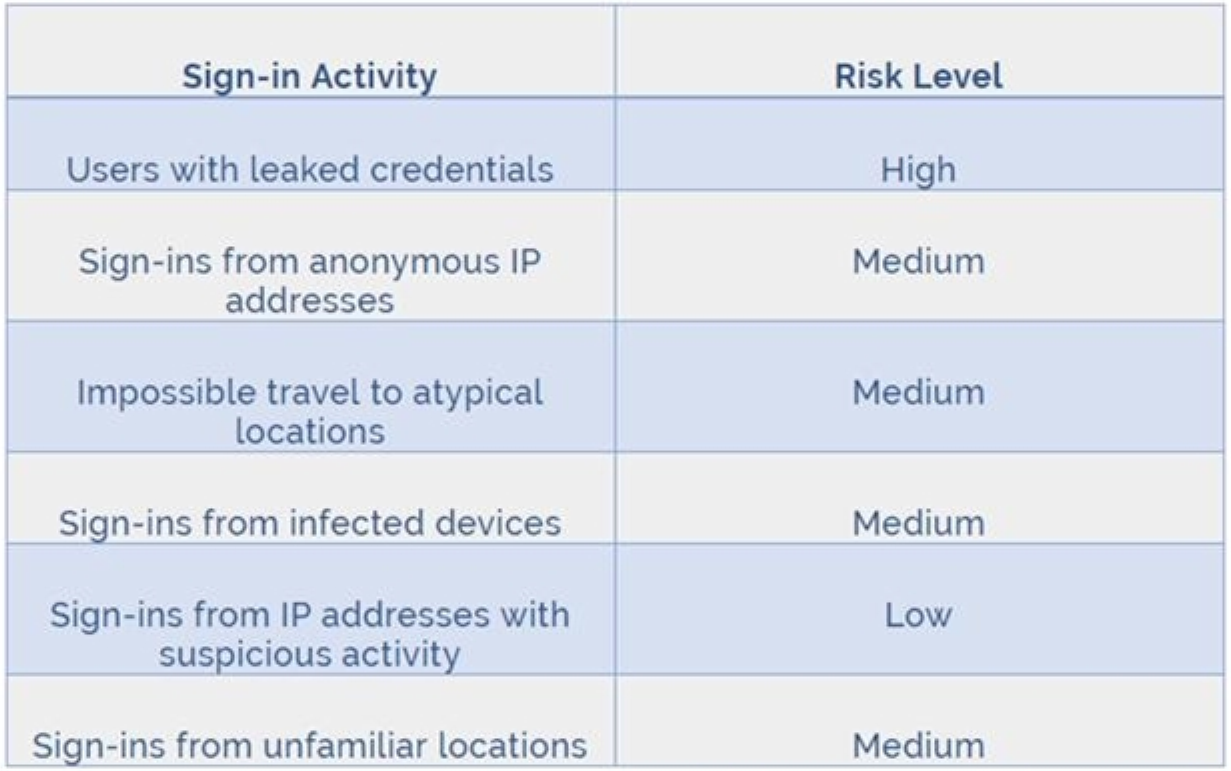
Answer Area:



Answer Area

Statements	Yes	No
If User1 signs in from an unfamiliar location, he must change his password.	[✓ ○]	○
If User2 signs in from an anonymous IP address, she must change her password.	[✓ ○]	○
If User3 signs in from a computer containing malware that is communicating with known bot servers, he must change his password.	○	[✓ ○]

Section:
Explanation:
Box 1: Yes
User1 is member of Group1. Sign in from unfamiliar location is risk level Medium.
Box 2: Yes
User2 is member of Group1. Sign in from anonymous IP address is risk level Medium.
Box 3: No
Sign-ins from IP addresses with suspicious activity is low.
Note:

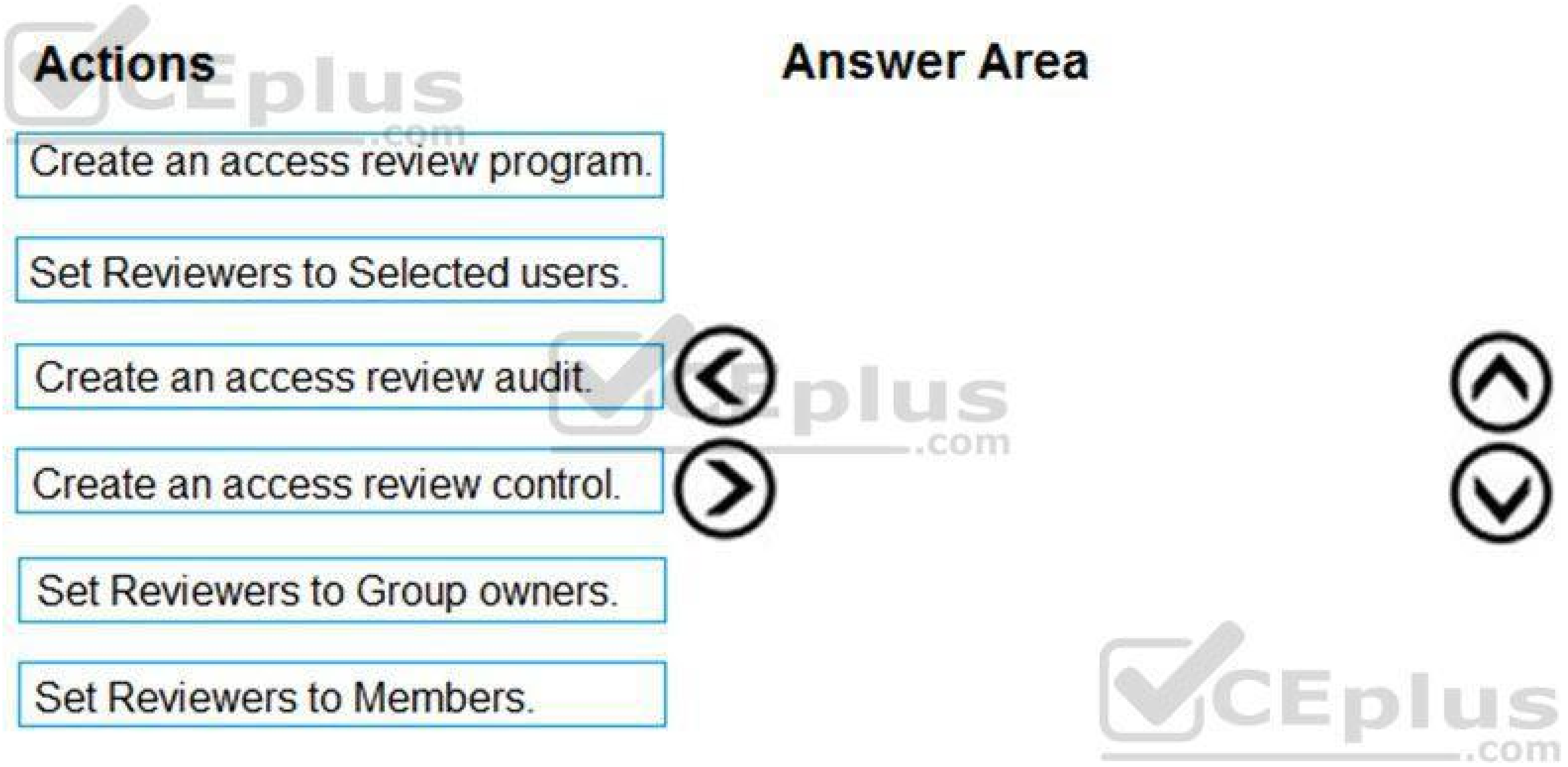


Sign-in Activity	Risk Level
Users with leaked credentials	High
Sign-ins from anonymous IP addresses	Medium
Impossible travel to atypical locations	Medium
Sign-ins from infected devices	Medium
Sign-ins from IP addresses with suspicious activity	Low
Sign-ins from unfamiliar locations	Medium

Azure AD Identity protection can detect six types of suspicious sign-in activities:
Users with leaked credentials
Sign-ins from anonymous IP addresses
Impossible travel to atypical locations
Sign-ins from infected devices
Sign-ins from IP addresses with suspicious activity
Sign-ins from unfamiliar locations
These six types of events are categorized in to 3 levels of risks – High, Medium & Low:
References:
http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/

QUESTION 23
DRAG DROP
You need to configure an access review. The review will be assigned to a new collection of reviews and reviewed by resource owners.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

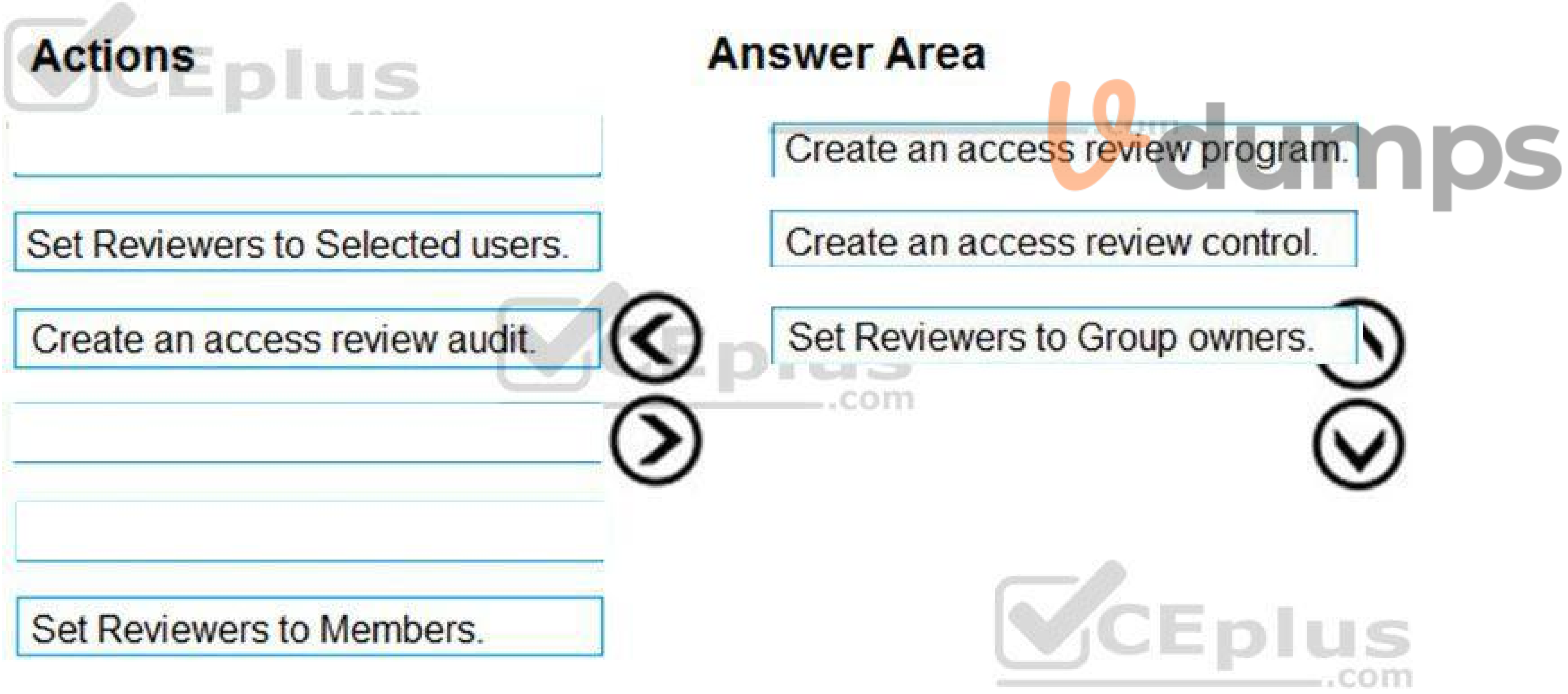


Actions

- Create an access review program.
- Set Reviewers to Selected users.
- Create an access review audit.
- Create an access review control.
- Set Reviewers to Group owners.
- Set Reviewers to Members.

Answer Area

Correct Answer:



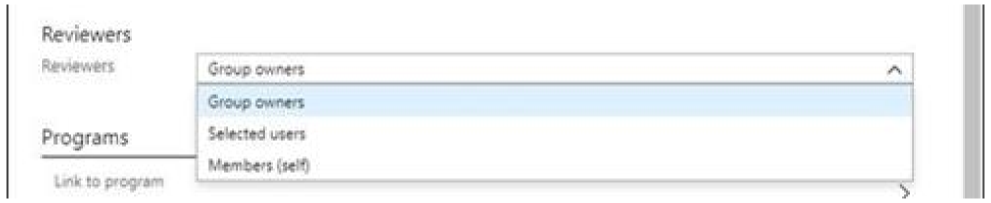
Actions

- Set Reviewers to Selected users.
- Create an access review audit.
- Set Reviewers to Members.

Answer Area

- Create an access review program.
- Create an access review control.
- Set Reviewers to Group owners.

Section:
Explanation:
Step 1: Create an access review program
Step 2: Create an access review control
Step 3: Set Reviewers to Group owners
In the Reviewers section, select either one or more people to review all the users in scope. Or you can select to have the members review their own access. If the resource is a group, you can ask the group owners to review.



Reviewers

Reviewers: Group owners

Programs

Link to program

References:
https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review
https://docs.microsoft.com/en-us/azure/active-directory/governance/manage-programs-controls

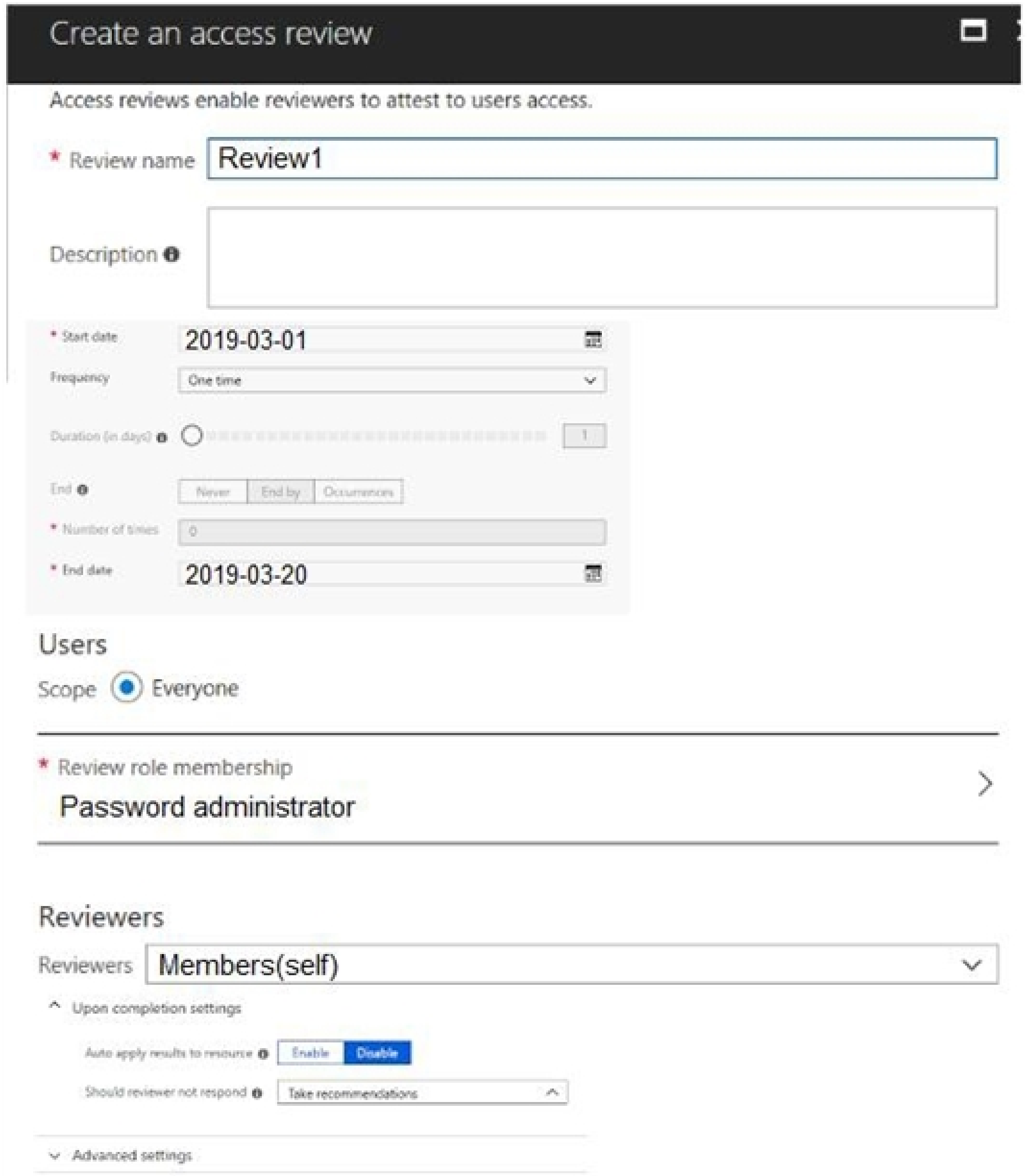
QUESTION 24

HOTSPOT

You have an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Role	Sign in frequency
User1	Password administrator	Sign in every work day
User2	Password administrator	Sign in bi-weekly
User3	Global administrator, Password administrator	Signs in every month

You configure an access review named Review1 as shown in the following exhibit.



Create an access review

Access reviews enable reviewers to attest to users access.

* Review name: Review1

Description:

* Start date: 2019-03-01

Frequency: One time

Duration (in days): 1

* Number of times: 0

* End date: 2019-03-20

Users

Scope: ● Everyone

* Review role membership: Password administrator

Reviewers

Reviewers: Members(self)

Upon completion settings

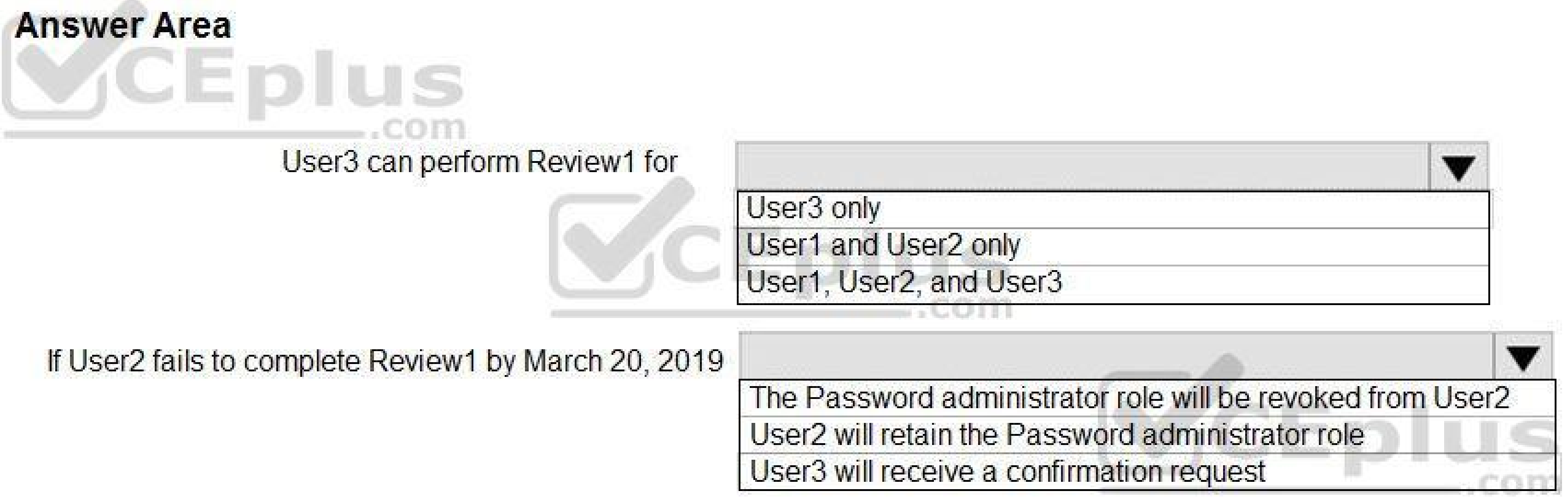
Auto apply results to resource: Disable

Should reviewer not respond: Take recommendations

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

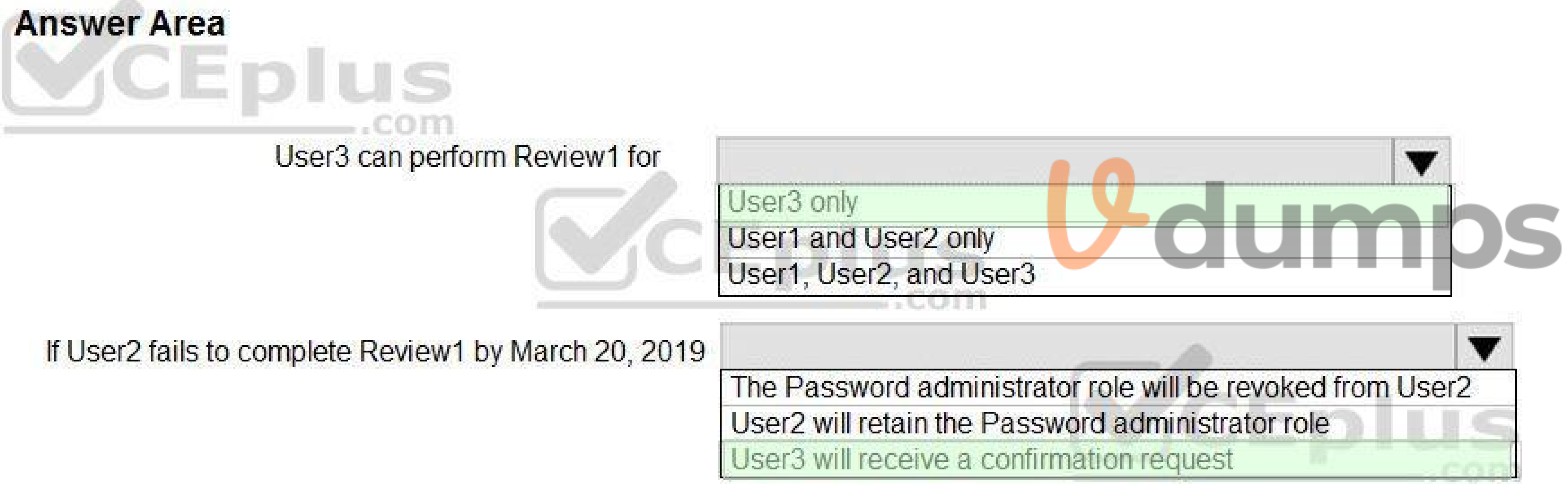


Answer Area

User3 can perform Review1 for ▼
- User3 only
- User1 and User2 only
- User1, User2, and User3

If User2 fails to complete Review1 by March 20, 2019 ▼
- The Password administrator role will be revoked from User2
- User2 will retain the Password administrator role
- User3 will receive a confirmation request

Answer Area:



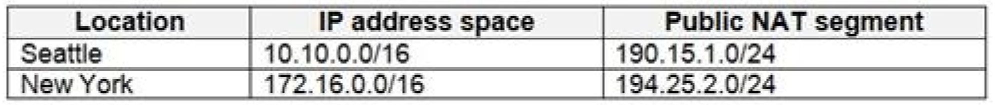
Answer Area

User3 can perform Review1 for ▼
- [✓ User3 only]
- User1 and User2 only
- User1, User2, and User3

If User2 fails to complete Review1 by March 20, 2019 ▼
- The Password administrator role will be revoked from User2
- User2 will retain the Password administrator role
- [✓ User3 will receive a confirmation request]

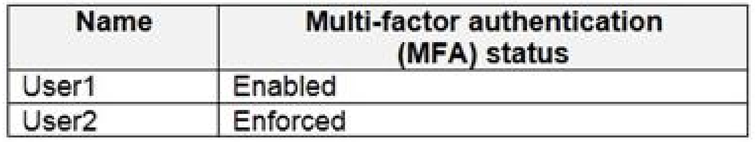
Section:
Explanation:
Box 1: User3 only
Use the Members (self) option to have the users review their own role assignments.
Box 2: User3 will receive a confirmation request
Use the Should reviewer not respond list to specify what happens for users that are not reviewed by the reviewer within the review period. This setting does not impact users who have been reviewed by the reviewers manually. If the final reviewer's decision is Deny, then the user's access will be removed.
No change - Leave user's access unchanged
Remove access - Remove user's access
Approve access - Approve user's access
Take recommendations - Take the system's recommendation on denying or approving the user's continued access
References:
https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-how-to-start-security-review

QUESTION 25
HOTSPOT
Your company has two offices in Seattle and New York. Each office connects to the Internet by using a NAT device. The offices use the IP addresses shown in the following table.



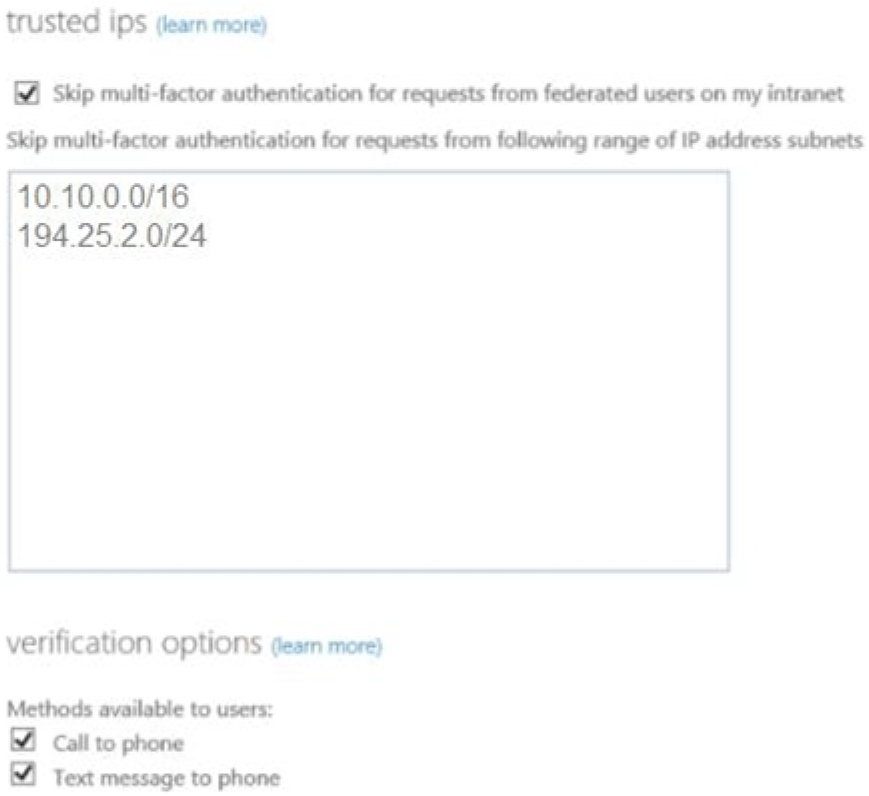
Location	IP address space	Public NAT segment
Seattle	10.10.0.0/16	190.15.1.0/24
New York	172.16.0.0/16	194.25.2.0/24

The company has an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.



Name	Multi-factor authentication (MFA) status
User1	Enabled
User2	Enforced

The MFA service settings are configured as shown in the exhibit. (Click the Exhibit tab.)



trusted ips (learn more)

☑ Skip multi-factor authentication for requests from federated users on my intranet

Skip multi-factor authentication for requests from following range of IP address subnets

```
10.10.0.0/16
194.25.2.0/24
```

verification options (learn more)

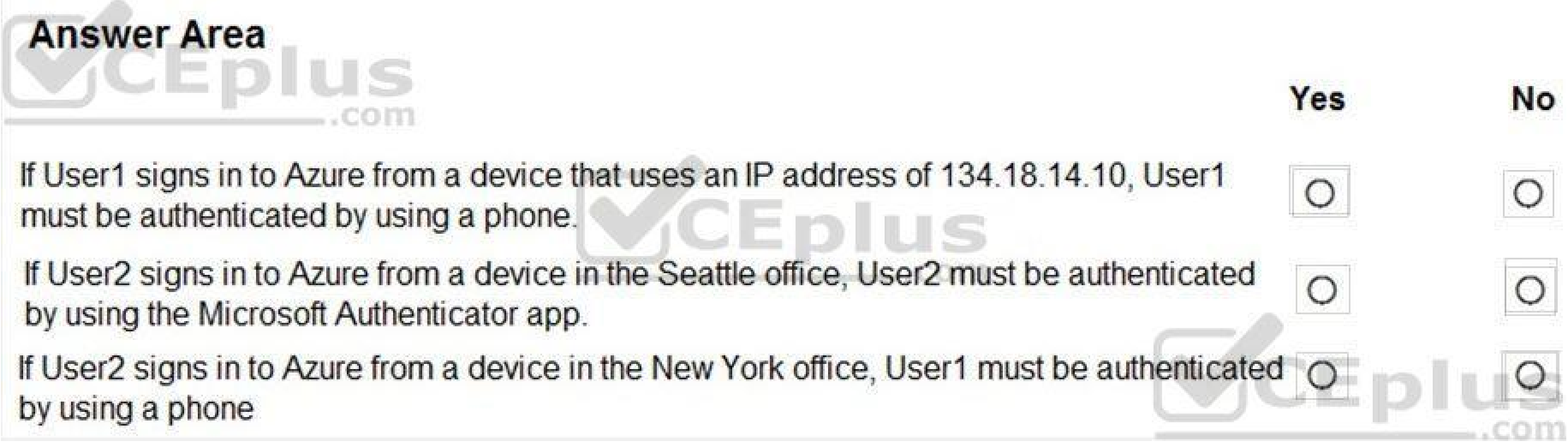
Methods available to users:

☑ Call to phone

☑ Text message to phone

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

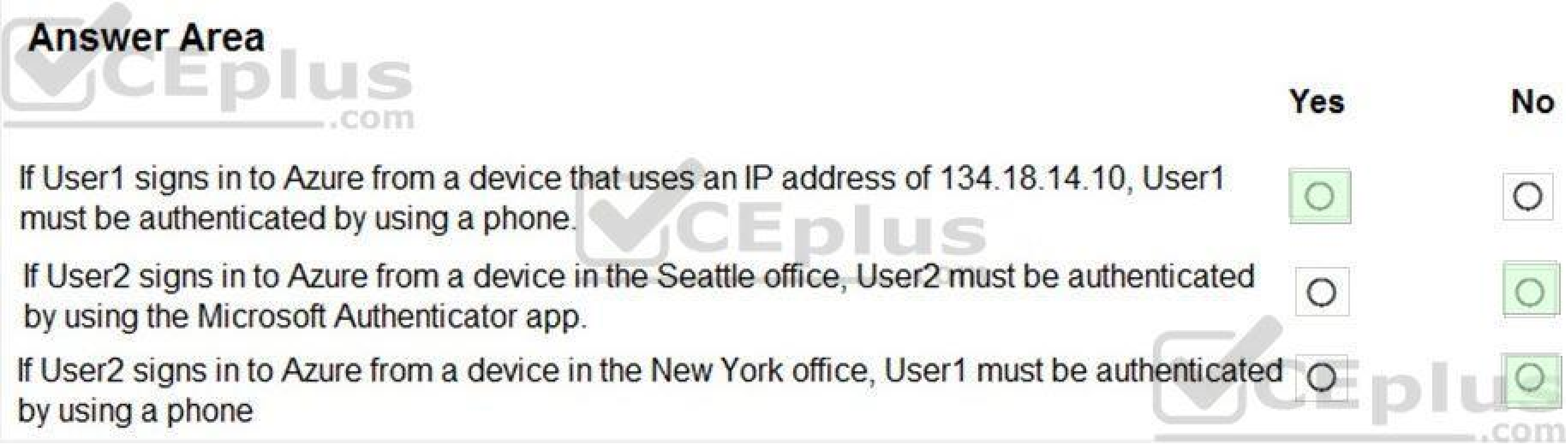
Hot Area:



Answer Area

	Yes	No
If User1 signs in to Azure from a device that uses an IP address of 134.18.14.10, User1 must be authenticated by using a phone.	○	○
If User2 signs in to Azure from a device in the Seattle office, User2 must be authenticated by using the Microsoft Authenticator app.	○	○
If User2 signs in to Azure from a device in the New York office, User1 must be authenticated by using a phone	○	○

Answer Area:



Answer Area

	Yes	No
If User1 signs in to Azure from a device that uses an IP address of 134.18.14.10, User1 must be authenticated by using a phone.	[✓ ○]	○
If User2 signs in to Azure from a device in the Seattle office, User2 must be authenticated by using the Microsoft Authenticator app.	○	[✓ ○]
If User2 signs in to Azure from a device in the New York office, User1 must be authenticated by using a phone	○	[✓ ○]

Section:

Explanation:

Box 2: No

Use of Microsoft Authenticator is not required.

Note: Microsoft Authenticator is a multifactor app for mobile devices that generates time-based codes used during the Two-Step Verification process.

Box 3: No

The New York IP address subnet is included in the "skip multi-factor authentication for request.

References:

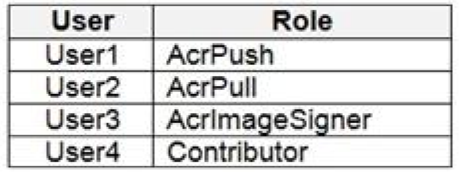
https://www.cayosoft.com/difference-enabling-enforcing-mfa/

QUESTION 26

HOTSPOT

You have an Azure Container Registry named Registry1.

You add role assignment for Registry1 as shown in the following table.

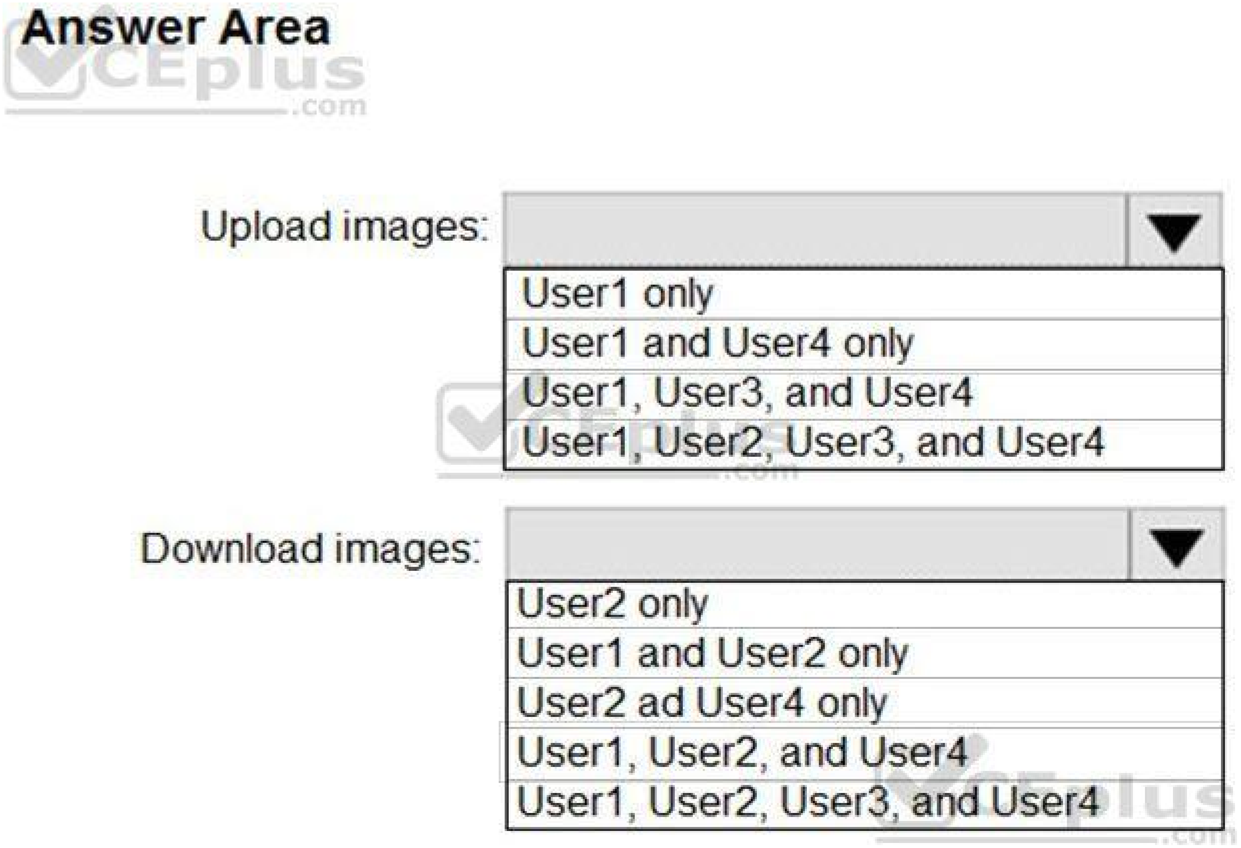


User	Role
User1	AcrPush
User2	AcrPull
User3	AcrImageSigner
User4	Contributor

Which users can upload images to Registry1 and download images from Registry1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

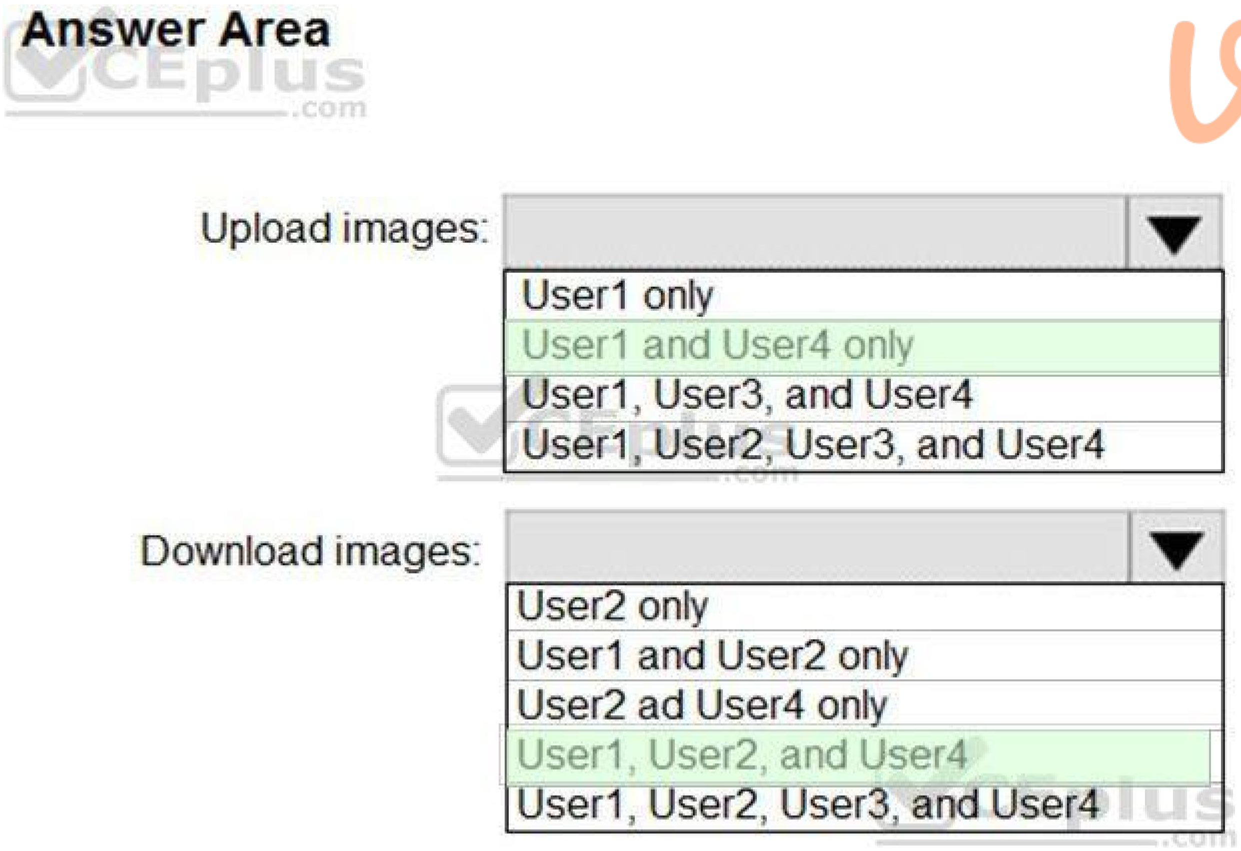
Upload images:

- User1 only
- User1 and User4 only
- User1, User3, and User4
- User1, User2, User3, and User4

Download images:

- User2 only
- User1 and User2 only
- User2 ad User4 only
- User1, User2, and User4
- User1, User2, User3, and User4

Answer Area:



Answer Area

Upload images:

- User1 only
- [✓ User1 and User4 only]
- User1, User3, and User4
- User1, User2, User3, and User4

Download images:

- User2 only
- User1 and User2 only
- User2 ad User4 only
- [✓ User1, User2, and User4]
- User1, User2, User3, and User4

Section:

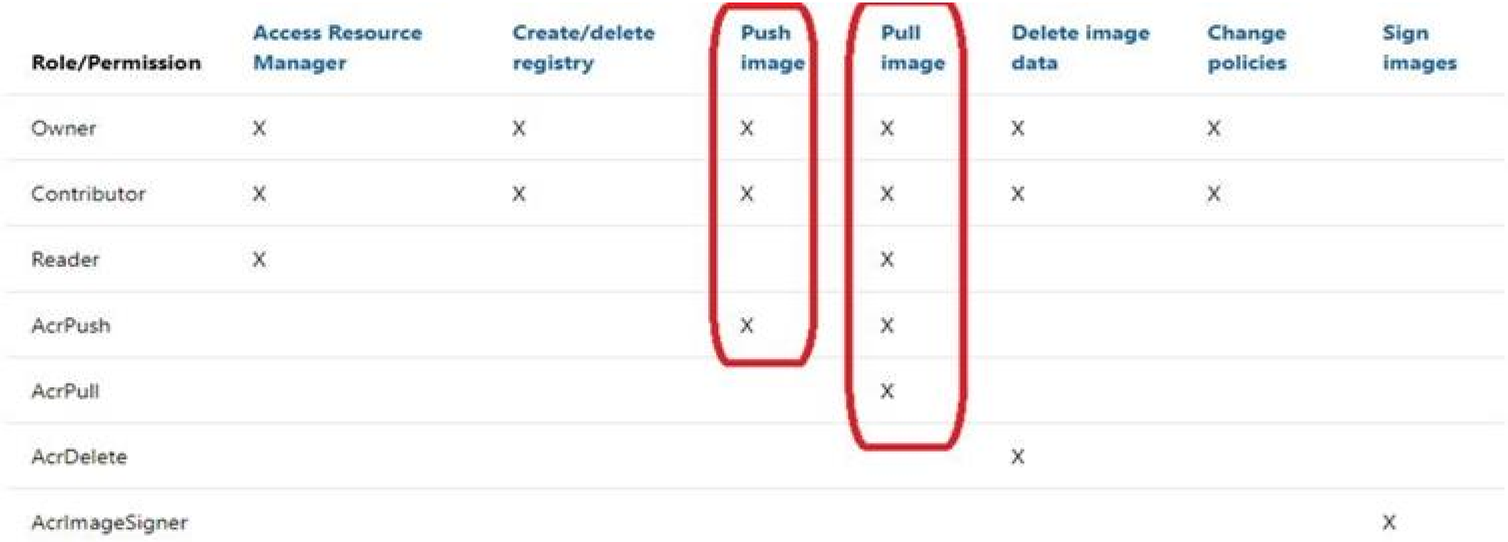
Explanation:

Box 1: User1 and User4 only

Owner, Contributor and AcrPush can push images.

Box 2: User1, User2, and User4

All, except AcrImagineSigner, can download/pull images.



Role/Permission	Access Resource Manager	Create/delete registry	Push image	Pull image	Delete image data	Change policies	Sign images
Owner	X	X	X	X	X	X	
Contributor	X	X	X	X	X	X	
Reader	X			X			
AcrPush			X	X			
AcrPull				X			
AcrDelete					X		
AcrImageSigner							X

References:
https://docs.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-roles

QUESTION 27

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You have a hybrid configuration of Azure Active Directory (Azure AD).
You have an Azure HDInsight cluster on a virtual network.
You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials.
You need to configure the environment to support the planned authentication.
Solution: You deploy Azure Active Directory Domain Services (Azure AD DS) to the Azure subscription.
Does this meet the goal?

A. Yes

B. No

Correct Answer: B
Section:
Explanation:
Instead, you connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.
Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions:
Create Azure Virtual Network.
Create a custom DNS server in the Azure Virtual Network.
Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver. Configure forwarding between the custom DNS server and your on-premises DNS server.
References:
https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network

QUESTION 28

Your network contains an Active Directory forest named contoso.com. You have an Azure Active Directory (Azure AD) tenant named contoso.com.
You plan to configure synchronization by using the Express Settings installation option in Azure AD Connect.
You need to identify which roles and groups are required to perform the planned configurations. The solution must use the principle of least privilege.
Which two roles and groups should you identify? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. the Domain Admins group in Active Directory

B. the Security administrator role in Azure AD

C. the Global administrator role in Azure AD

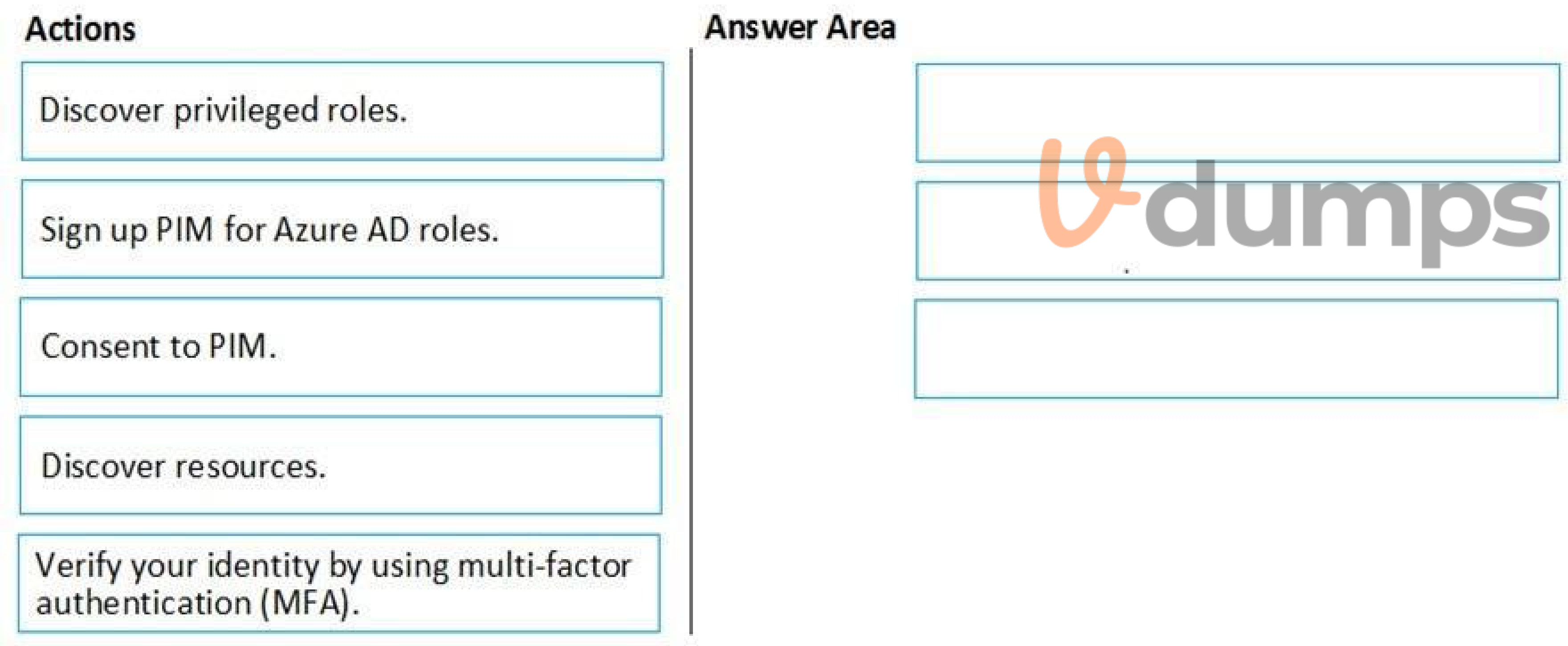
D. the User administrator role in Azure AD

E. the Enterprise Admins group in Active Directory

Correct Answer: C, E
Section:
Explanation:
References:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-accounts-permissions

QUESTION 29
DRAG DROP
You create an Azure subscription with Azure AD Premium P2.
You need to ensure that you can use Azure Active Directory (Azure AD) Privileged Identity Management (PIM) to secure Azure roles.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Actions

Discover privileged roles.

Sign up PIM for Azure AD roles.

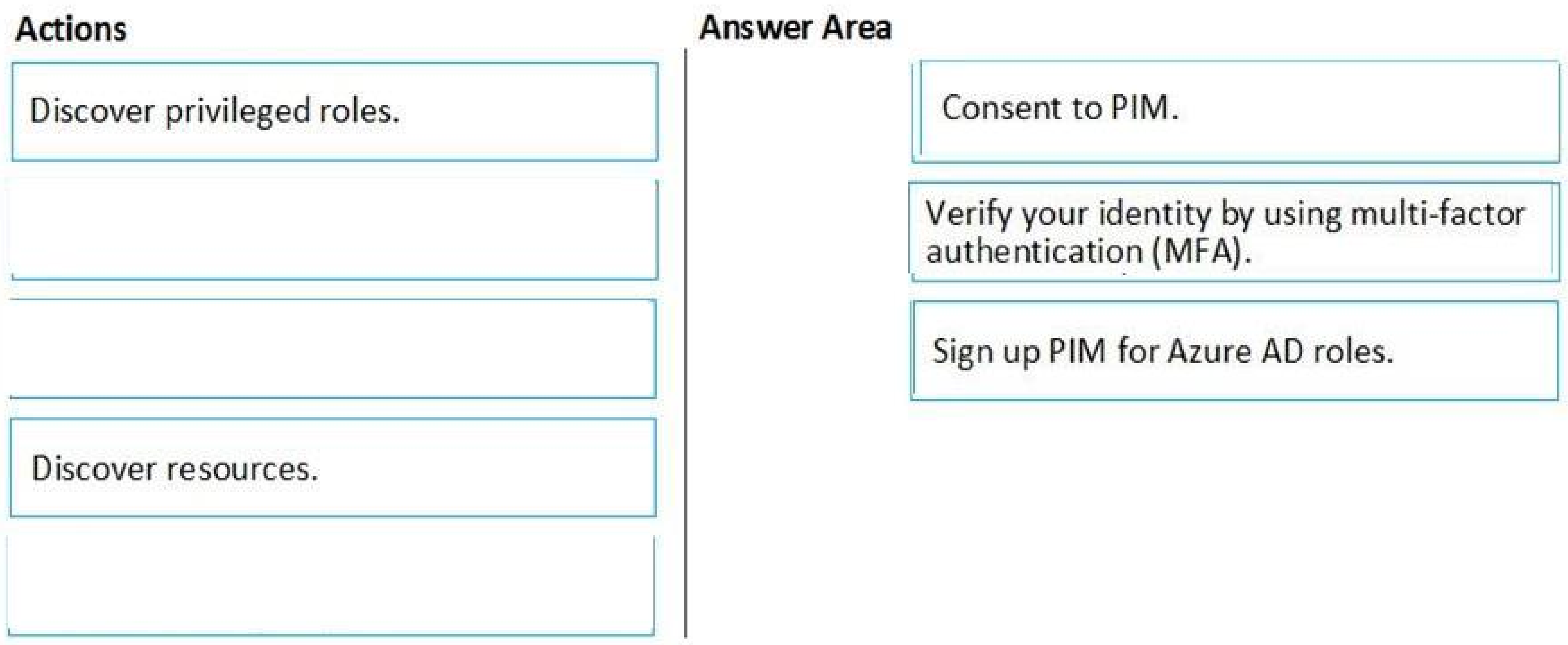
Consent to PIM.

Discover resources.

Verify your identity by using multi-factor authentication (MFA).

Answer Area

Correct Answer:



Actions

Discover privileged roles.

Discover resources.

Answer Area

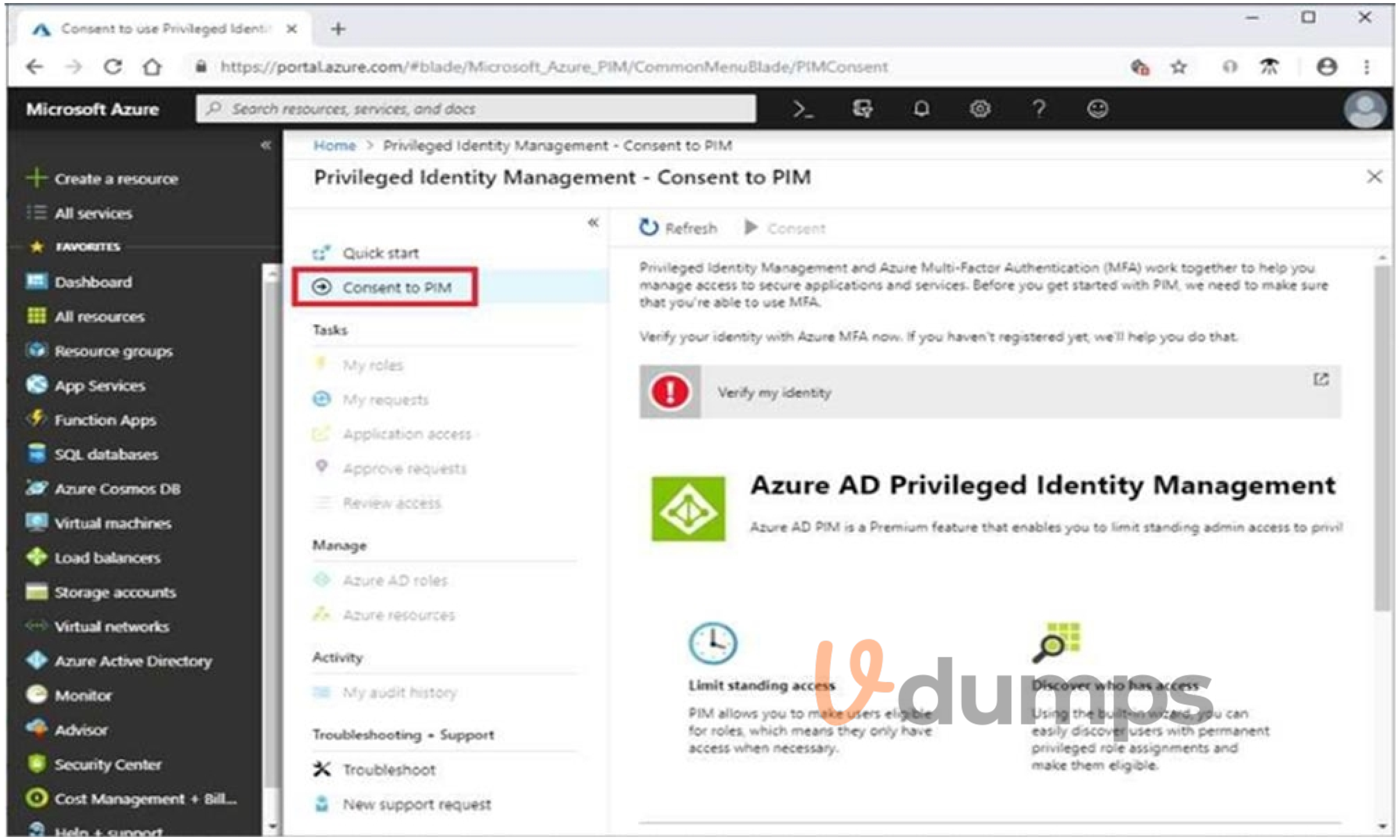
Consent to PIM.

Verify your identity by using multi-factor authentication (MFA).

Sign up PIM for Azure AD roles.

Section:

Explanation:



Privileged Identity Management - Consent to PIM

Privileged Identity Management and Azure Multi-Factor Authentication (MFA) work together to help you manage access to secure applications and services. Before you get started with PIM, we need to make sure that you're able to use MFA.

Verify your identity with Azure MFA now. If you haven't registered yet, we'll help you do that.

Azure AD Privileged Identity Management

Azure AD PIM is a Premium feature that enables you to limit standing admin access to privil

Limit standing access

PIM allows you to make users eligible for roles, which means they only have access when necessary.

Discover who has access

Using the built-in wizard, you can easily discover users with permanent privileged role assignments and make them eligible.

Step: 2 Verify your identity by using multi-factor authentication (MFA)
Click Verify my identity to verify your identity with Azure MF
You'll be asked to pick an account.
Step 3: Sign up PIM for Azure AD roles
Once you have enabled PIM for your directory, you'll need to sign up PIM to manage Azure AD roles.

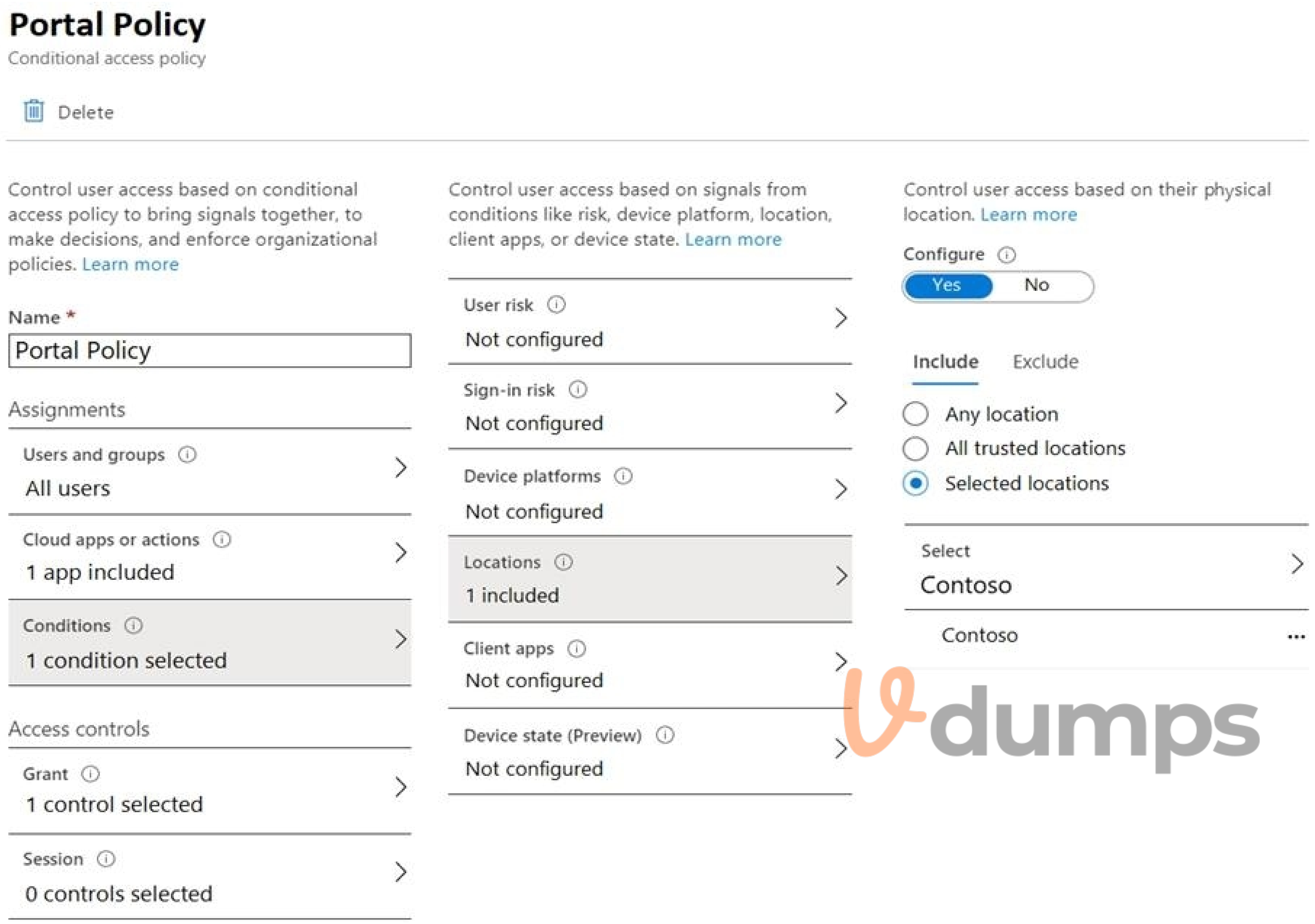
QUESTION 30

HOTSPOT

You create a new Azure subscription that is associated to a new Azure Active Directory (Azure AD) tenant.

You create one active conditional access policy named Portal Policy. Portal Policy is used to provide access to the Microsoft Azure Management cloud app.

The Conditions settings for Portal Policy are configured as shown in the Conditions exhibit. (Click the Conditions tab.)



Portal Policy

Conditional access policy

Delete

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

Portal Policy

Assignments

Users and groups ⓘ
All users

Cloud apps or actions ⓘ
1 app included

Conditions ⓘ
1 condition selected

Access controls

Grant ⓘ
1 control selected

Session ⓘ
0 controls selected

Control user access based on signals from conditions like risk, device platform, location, client apps, or device state. Learn more

User risk ⓘ
Not configured

Sign-in risk ⓘ
Not configured

Device platforms ⓘ
Not configured

Locations ⓘ
1 included

Client apps ⓘ
Not configured

Device state (Preview) ⓘ
Not configured

Control user access based on their physical location. Learn more

Configure ⓘ

[✓ Yes] No

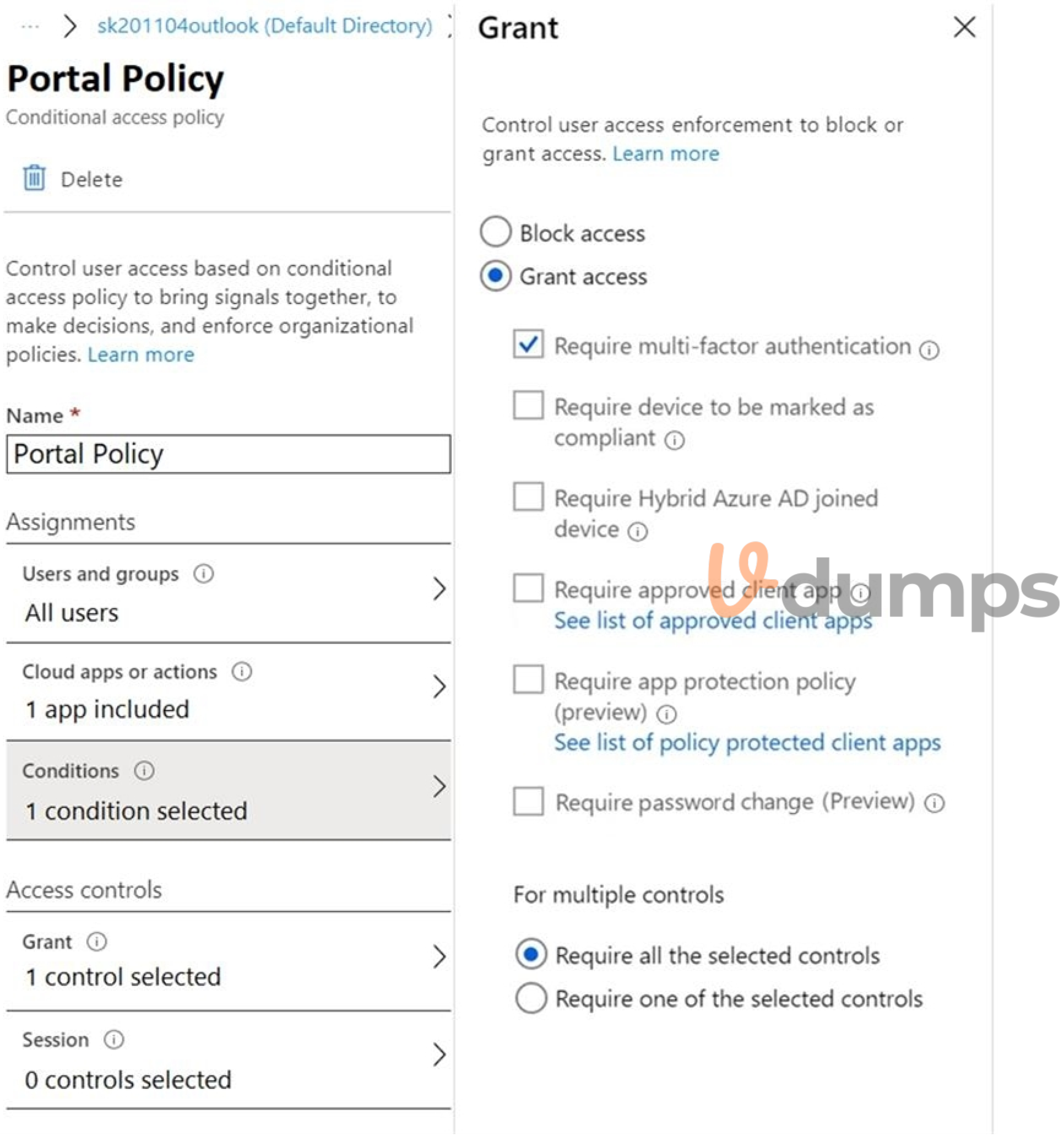
Include Exclude

○ Any location
○ All trusted locations
● Selected locations

Select
Contoso

Contoso ...

The Grant settings for Portal Policy are configured as shown in the Grant exhibit. (Click the Grant tab.)



··· > sk201104outlook (Default Directory)

Portal Policy

Conditional access policy

Delete

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

Portal Policy

Assignments

Users and groups: All users

Cloud apps or actions: 1 app included

Conditions: 1 condition selected

Access controls

Grant: 1 control selected

Session: 0 controls selected

Grant

Control user access enforcement to block or grant access. Learn more

○ Block access

● Grant access

☑ Require multi-factor authentication

□ Require device to be marked as compliant

□ Require Hybrid Azure AD joined device

□ Require approved client app
See list of approved client apps

□ Require app protection policy (preview)
See list of policy protected client apps

□ Require password change (Preview)

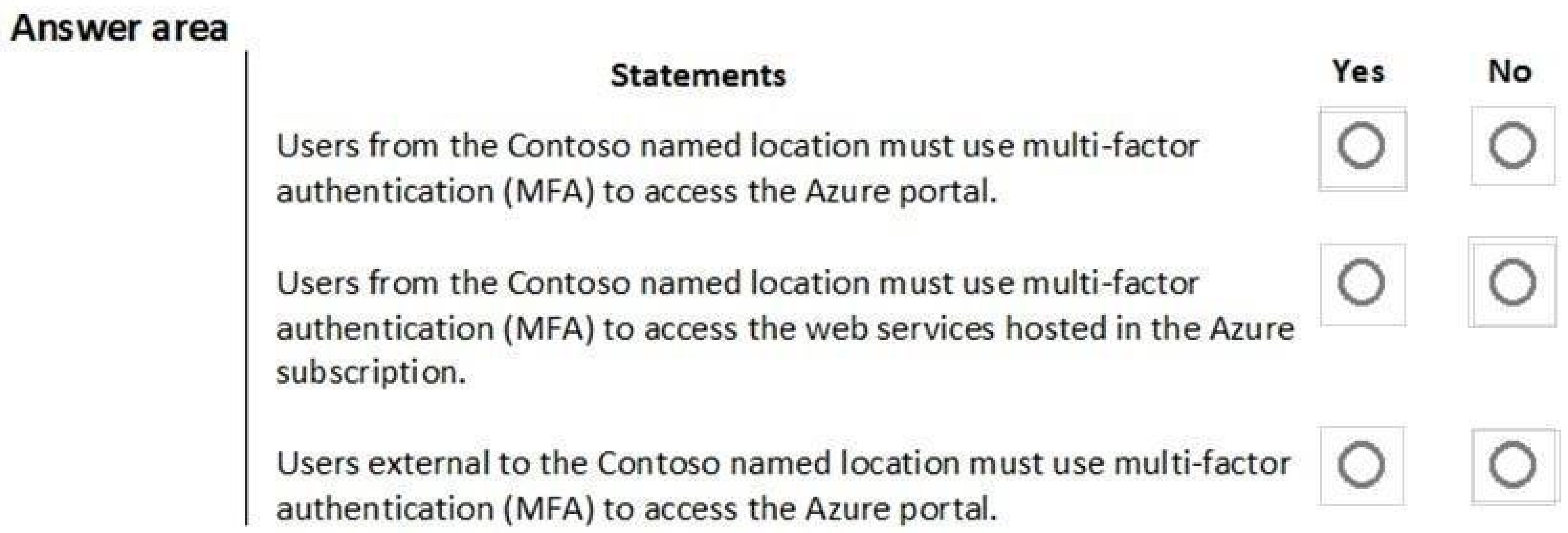
For multiple controls

● Require all the selected controls

○ Require one of the selected controls

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

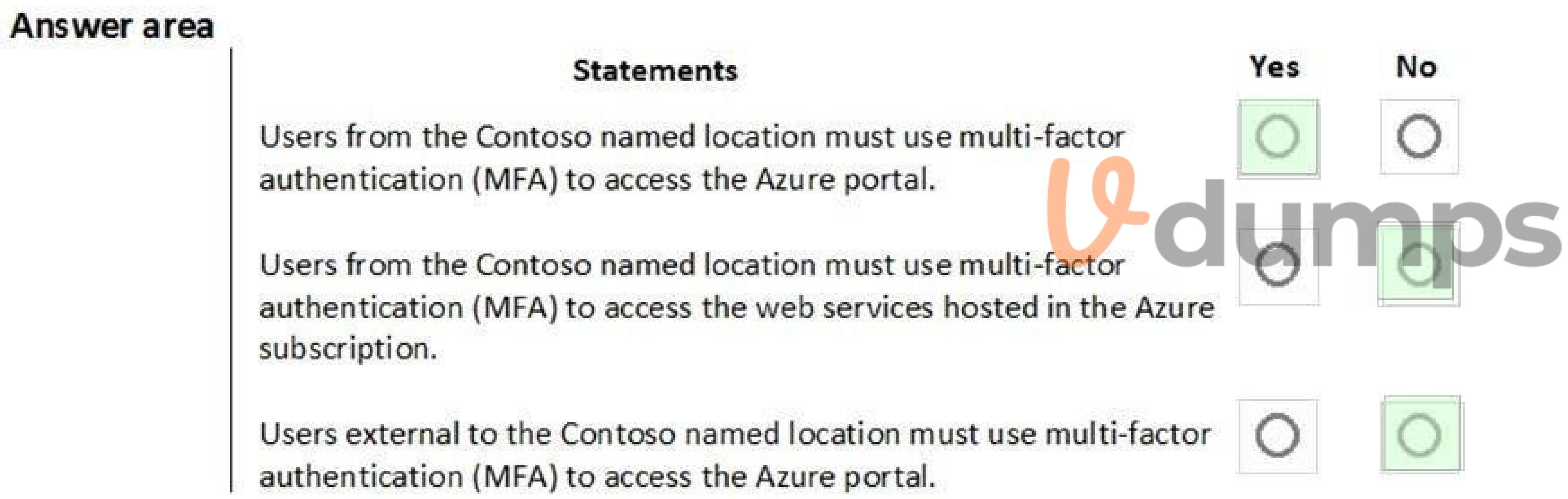
Hot Area:



Answer area

Statements	Yes	No
Users from the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.	○	○
Users from the Contoso named location must use multi-factor authentication (MFA) to access the web services hosted in the Azure subscription.	○	○
Users external to the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.	○	○

Answer Area:



Answer area

Statements	Yes	No
Users from the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.	[✓ ○]	○
Users from the Contoso named location must use multi-factor authentication (MFA) to access the web services hosted in the Azure subscription.	○	[✓ ○]
Users external to the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.	○	[✓ ○]

Section:
Explanation:
Box 1: Yes
The Contoso location is included in the policy and MFA is required.
Box 2: No
The policy applies to the Azure portal and Azure management endpoints. The policy does not apply to web services host in Azure.
Box 3: No
The policy applies only to users in the Contoso location. The policy does not apply to users external to the Contoso location.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

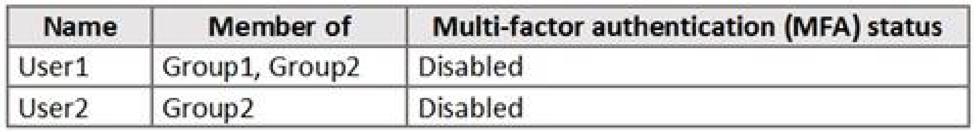
QUESTION 31
You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.
An administrator named Admin1 has access to the following identities:
An OpenID-enabled user account
A Hotmail account

An account in contoso.com
An account in an Azure AD tenant named fabrikam.com
You plan to use Azure Account Center to transfer the ownership of Sub1 to Admin1.
To which accounts can you transfer the ownership of Sub1?

A. contoso.com only
B. contoso.com, fabrikam.com, and Hotmail only
C. contoso.com and fabrikam.com only
D. contoso.com, fabrikam.com, Hotmail, and OpenID-enabled user account

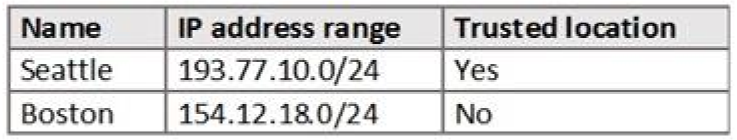
Correct Answer: C
Section:
Explanation:
When you transfer billing ownership of your subscription to an account in another Azure AD tenant, you can move the subscription to the new account's tenant. If you do so, all users, groups, or service principals who had role based access (RBAC) to manage subscriptions and its resources lose their access. Only the user in the new account who accepts your transfer request will have access to manage the resources.
Reference:
https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer
https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer#transferring-subscription-to-an-account-in-another-azure-ad-tenant

QUESTION 32
HOTSPOT
You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.



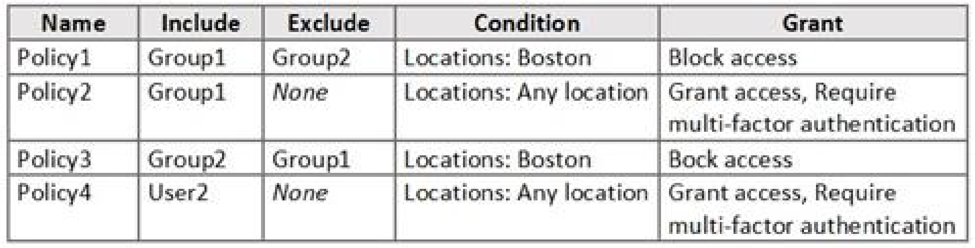
Name	Member of	Multi-factor authentication (MFA) status
User1	Group1, Group2	Disabled
User2	Group2	Disabled

The tenant contains the named locations shown in the following table.



Name	IP address range	Trusted location
Seattle	193.77.10.0/24	Yes
Boston	154.12.18.0/24	No

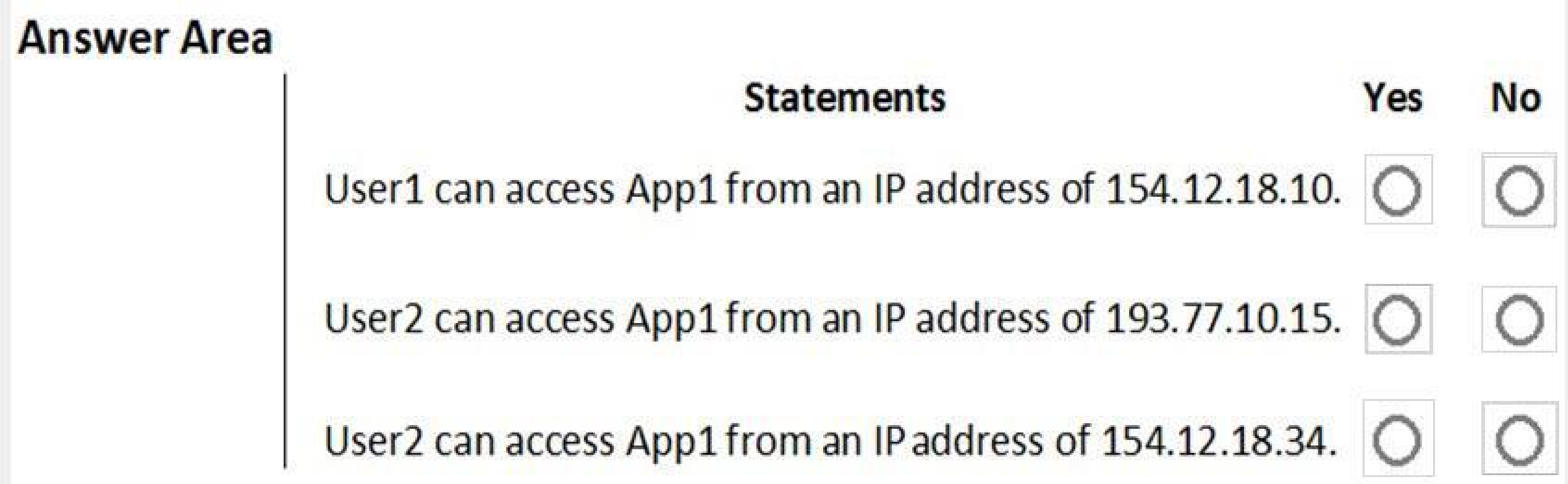
You create the conditional access policies for a cloud app named App1 as shown in the following table.



Name	Include	Exclude	Condition	Grant
Policy1	Group1	Group2	Locations: Boston	Block access
Policy2	Group1	*None*	Locations: Any location	Grant access, Require multi-factor authentication
Policy3	Group2	Group1	Locations: Boston	Bock access
Policy4	User2	*None*	Locations: Any location	Grant access, Require multi-factor authentication

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

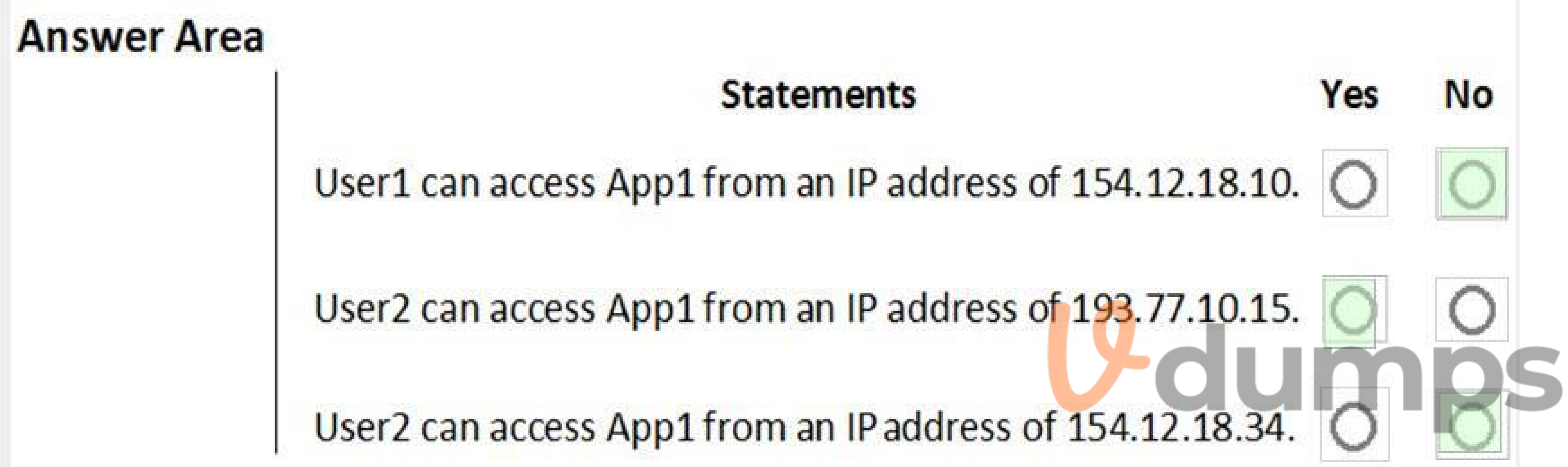
Hot Area:



Answer Area

Statements	Yes	No
User1 can access App1 from an IP address of 154.12.18.10.	○	○
User2 can access App1 from an IP address of 193.77.10.15.	○	○
User2 can access App1 from an IP address of 154.12.18.34.	○	○

Answer Area:

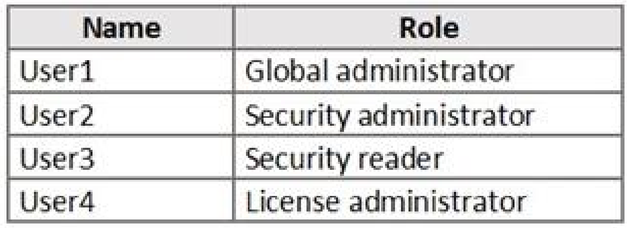


Answer Area

Statements	Yes	No
User1 can access App1 from an IP address of 154.12.18.10.	○	●
User2 can access App1 from an IP address of 193.77.10.15.	●	○
User2 can access App1 from an IP address of 154.12.18.34.	○	●

Section:
Explanation:

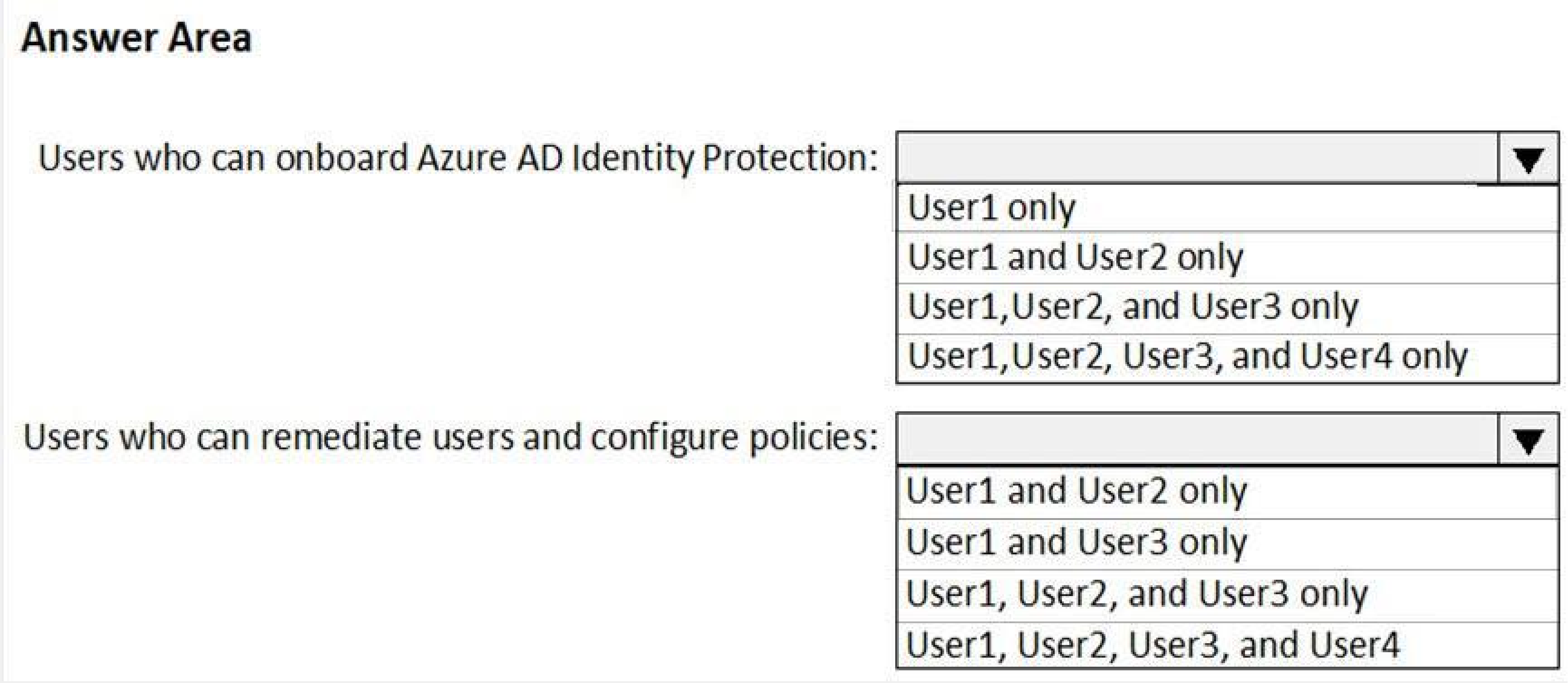
QUESTION 33
HOTSPOT
You have an Azure subscription named Sub 1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.



Name	Role
User1	Global administrator
User2	Security administrator
User3	Security reader
User4	License administrator

Each user is assigned an Azure AD Premium P2 license.
You plan to onboard and configure Azure AD Identity Protection.
Which users can onboard Azure AD Identity Protection, remediate users, and configure policies? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

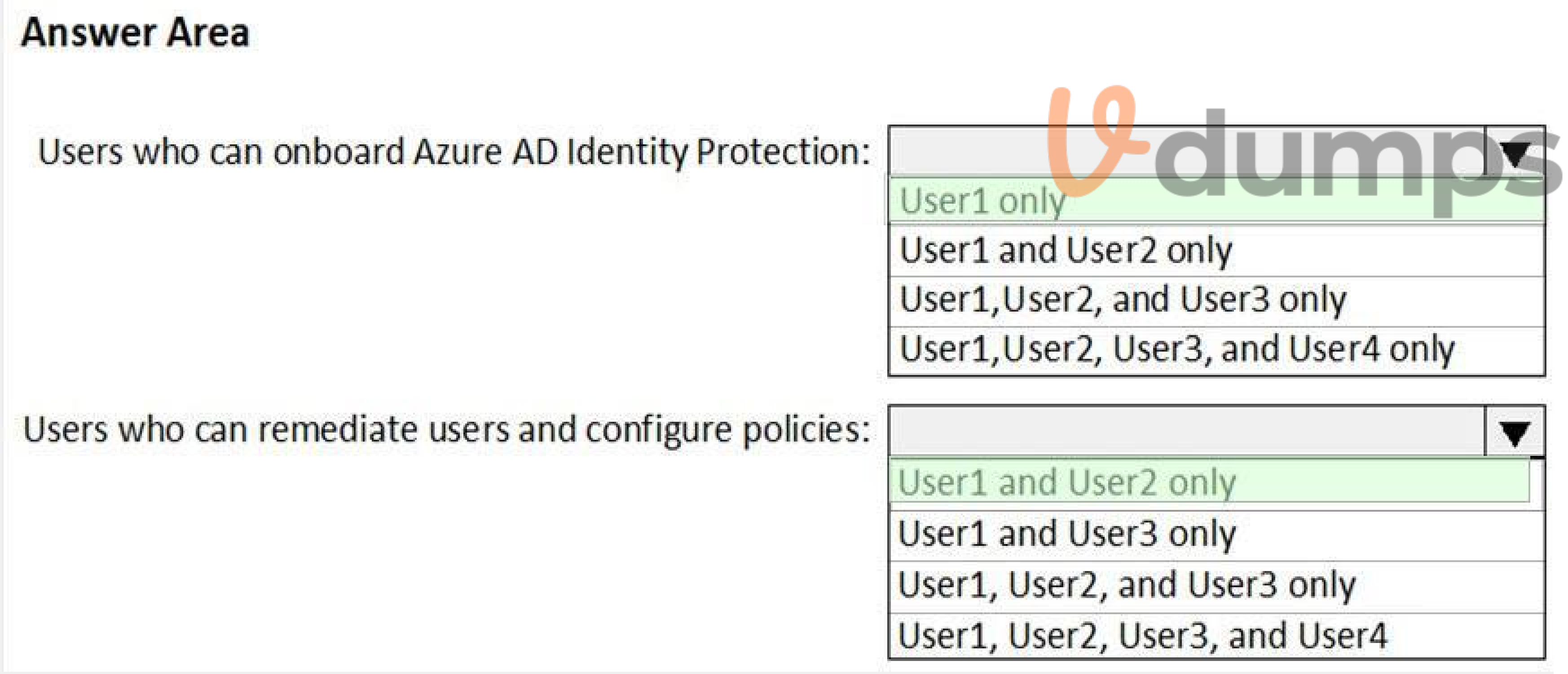
Users who can onboard Azure AD Identity Protection:

- User1 only
- User1 and User2 only
- User1,User2, and User3 only
- User1,User2, User3, and User4 only

Users who can remediate users and configure policies:

- User1 and User2 only
- User1 and User3 only
- User1, User2, and User3 only
- User1, User2, User3, and User4

Answer Area:



Answer Area

Users who can onboard Azure AD Identity Protection:

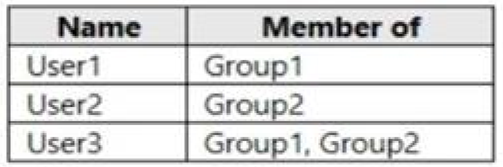
- [✓ User1 only]
- User1 and User2 only
- User1,User2, and User3 only
- User1,User2, User3, and User4 only

Users who can remediate users and configure policies:

- [✓ User1 and User2 only]
- User1 and User3 only
- User1, User2, and User3 only
- User1, User2, User3, and User4

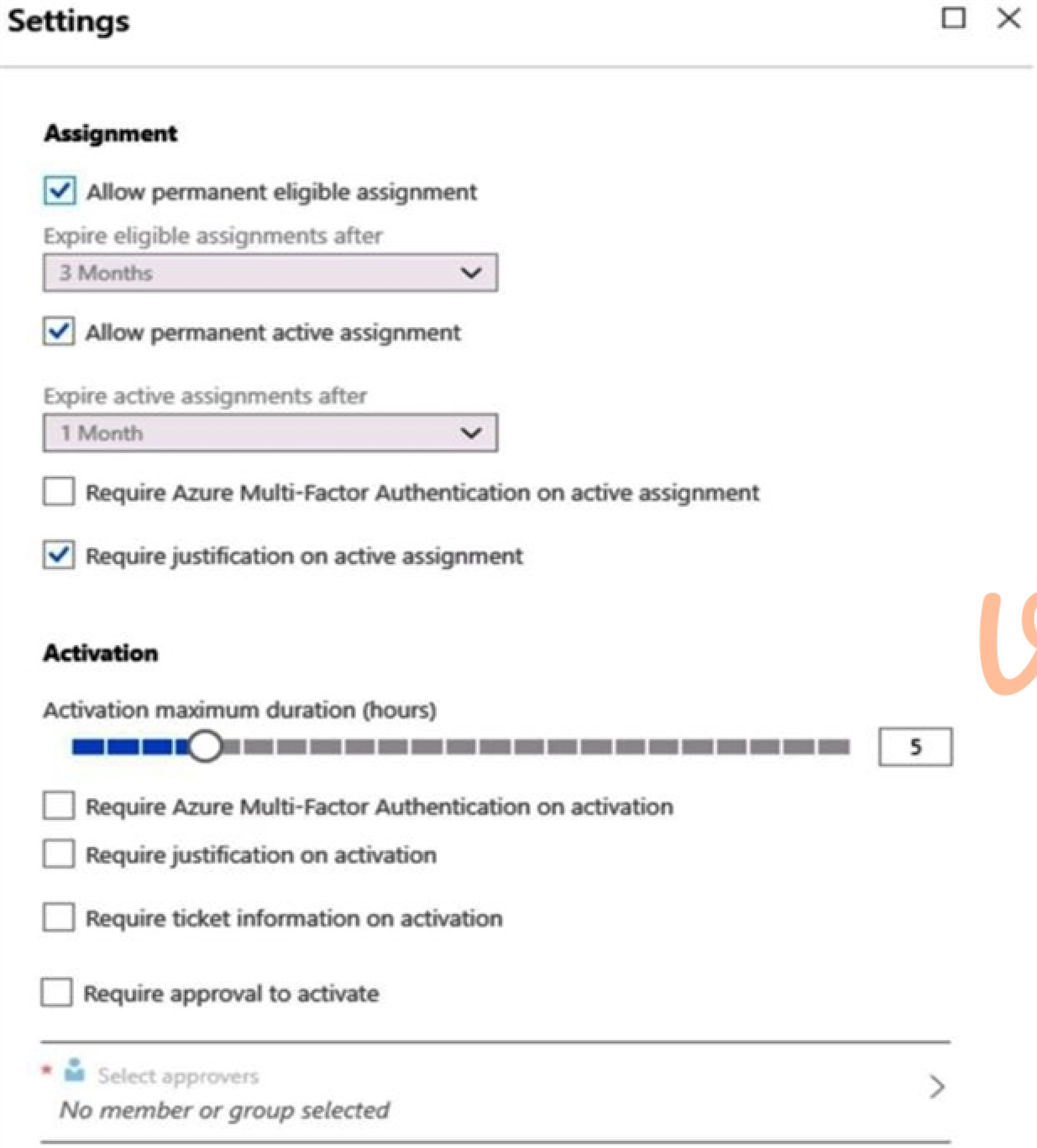
Section:
Explanation:

QUESTION 34
HOTSPOT
You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.



Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

From Azure AD Privileged Identity Management (PIM), you configure the settings for the Security Administrator role as shown in the following exhibit.



Settings

Assignment

☑ Allow permanent eligible assignment

Expire eligible assignments after

3 Months

☑ Allow permanent active assignment

Expire active assignments after

1 Month

□ Require Azure Multi-Factor Authentication on active assignment

☑ Require justification on active assignment

Activation

Activation maximum duration (hours)

5

□ Require Azure Multi-Factor Authentication on activation

□ Require justification on activation

□ Require ticket information on activation

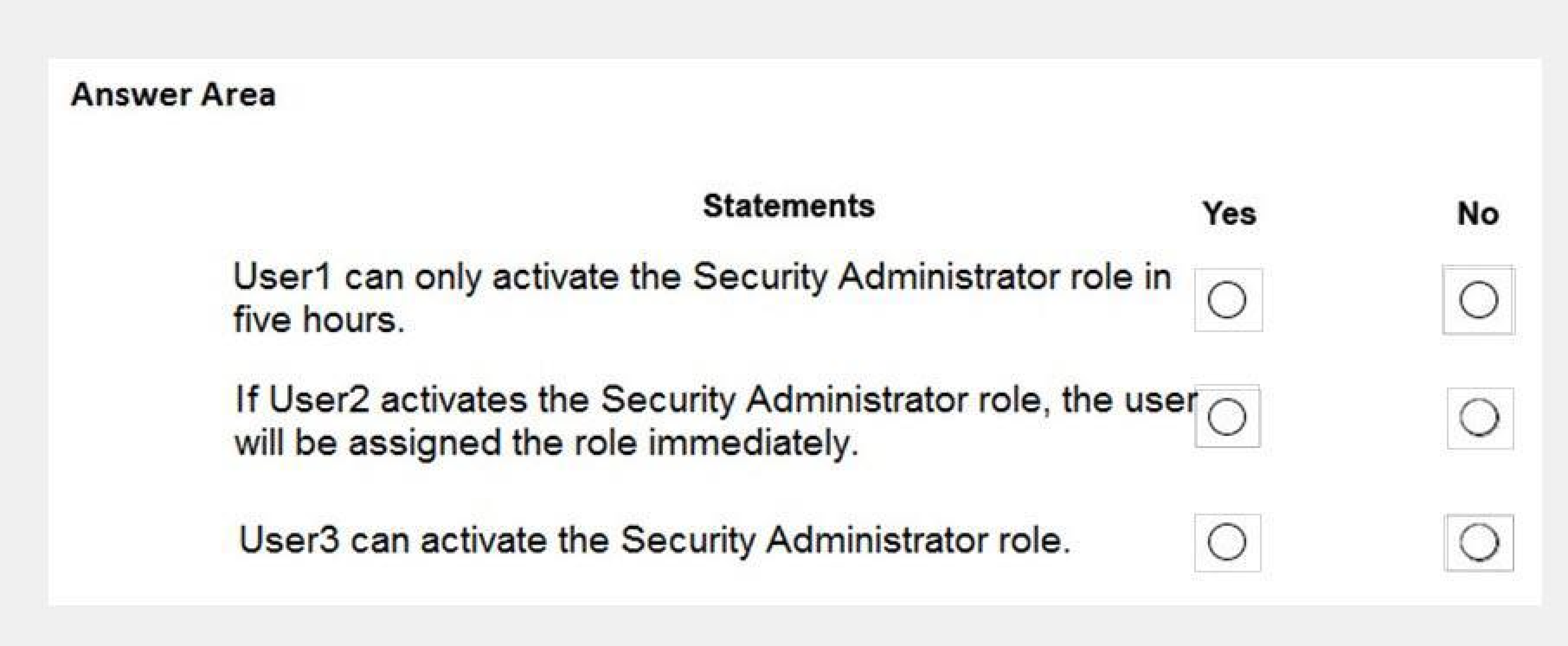
□ Require approval to activate

* Select approvers

No member or group selected

From PIM, you assign the Security Administrator role to the following groups:
Group1: Active assignment type, permanently assigned
Group2: Eligible assignment type, permanently eligible
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

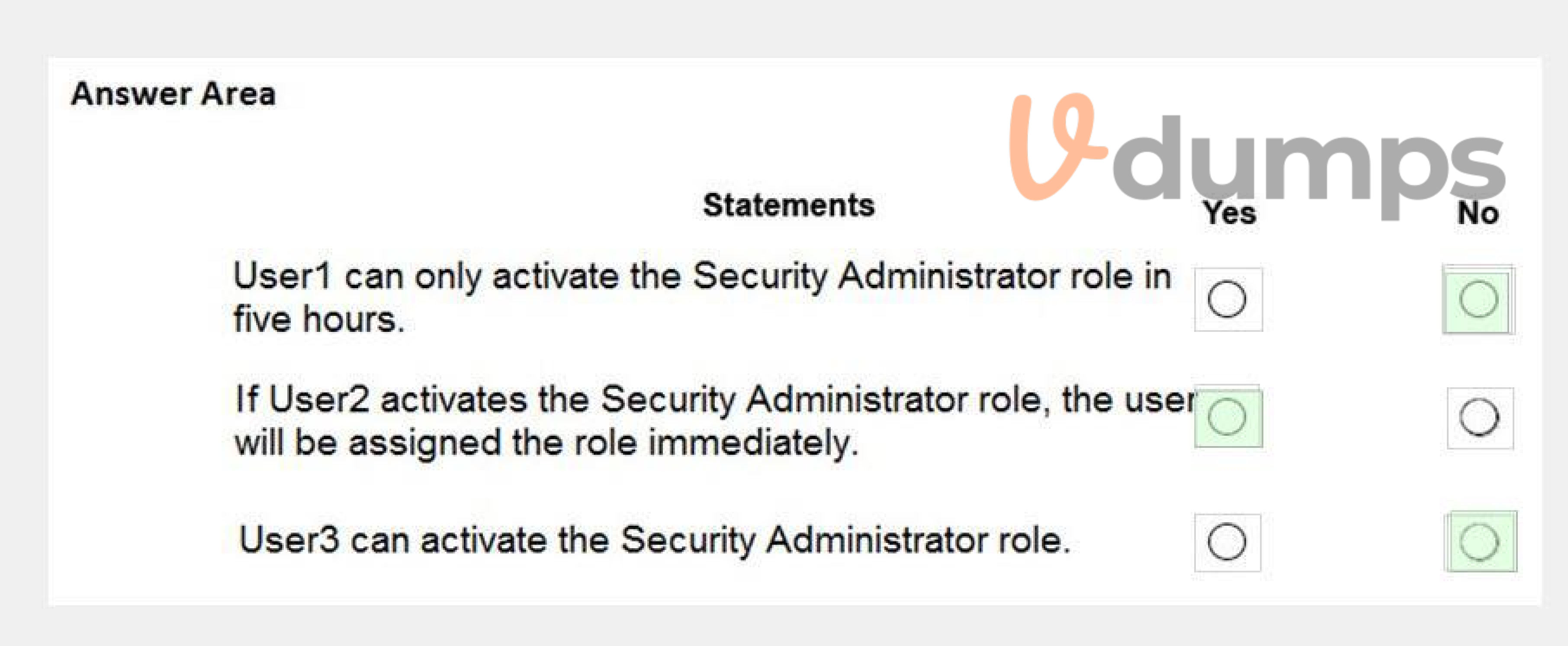
Hot Area:



Answer Area

Statements	Yes	No
User1 can only activate the Security Administrator role in five hours.	○	○
If User2 activates the Security Administrator role, the user will be assigned the role immediately.	○	○
User3 can activate the Security Administrator role.	○	○

Answer Area:



Answer Area

Statements	Yes	No
User1 can only activate the Security Administrator role in five hours.	○	[✓ ○]
If User2 activates the Security Administrator role, the user will be assigned the role immediately.	[✓ ○]	○
User3 can activate the Security Administrator role.	○	[✓ ○]

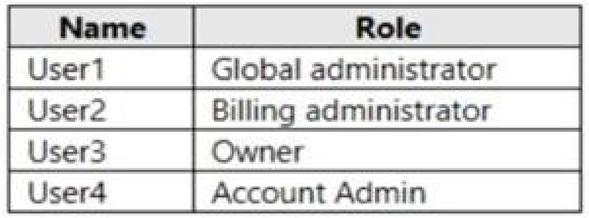
Section:
Explanation:
Box 1: No
User1 is a member of Group1. Group1: Active assignment type, permanently assigned
Box 2: Yes
Active Type: A role assignment that doesn't require a user to perform any action to use the role. Users assigned as active have the privileges assigned to the role
Box 3: No
User3 is member of Group1 and Group2.
Group1: Active assignment type, permanently assigned
Group2: Eligible assignment type, permanently eligible

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure https://docs.microsoft.com/bs-cyrl-ba/azure/active-directory/privileged-identity-management/pim-resource-roles-configure-role-settings

QUESTION 35

HOTSPOT

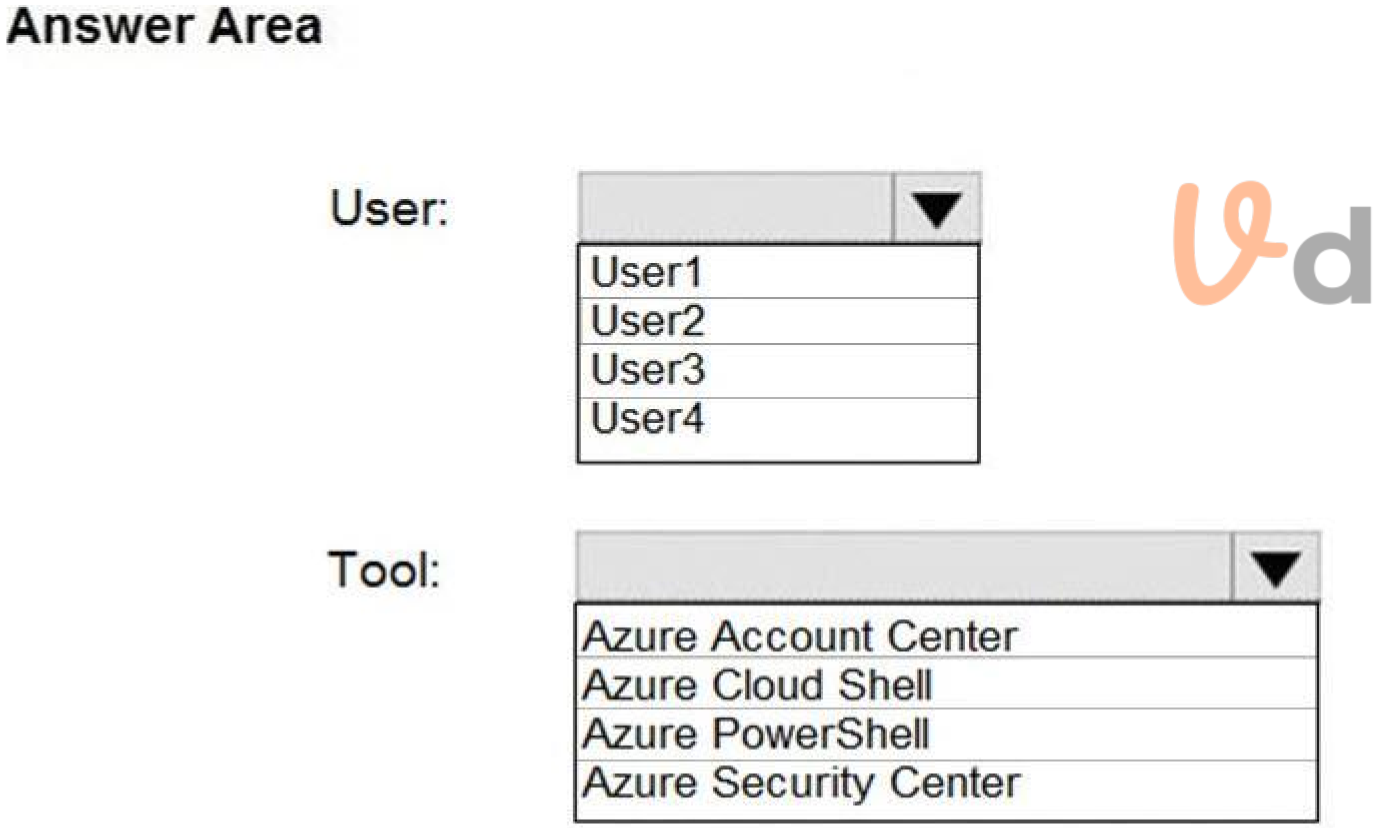
Your company has an Azure subscription named Subscription1 that contains the users shown in the following table.



Name	Role
User1	Global administrator
User2	Billing administrator
User3	Owner
User4	Account Admin

The company is sold to a new owner.
The company needs to transfer ownership of Subscription1.
Which user can transfer the ownership and which tool should the user use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:

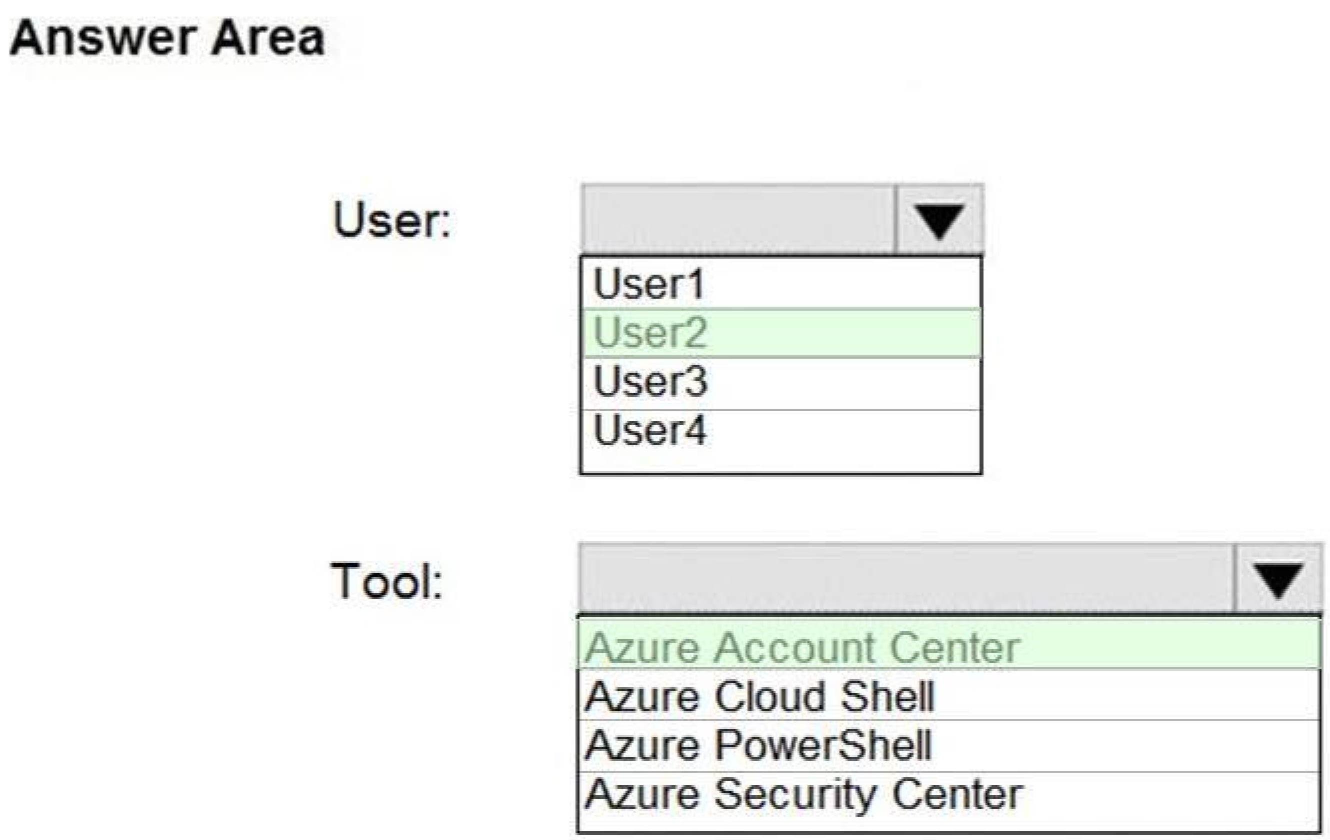


Answer Area

User:
- User1
- User2
- User3
- User4

Tool:
- Azure Account Center
- Azure Cloud Shell
- Azure PowerShell
- Azure Security Center

Answer Area:



Answer Area

User:

- User1
- [✓ User2]
- User3
- User4

Tool:

- [✓ Azure Account Center]
- Azure Cloud Shell
- Azure PowerShell
- Azure Security Center

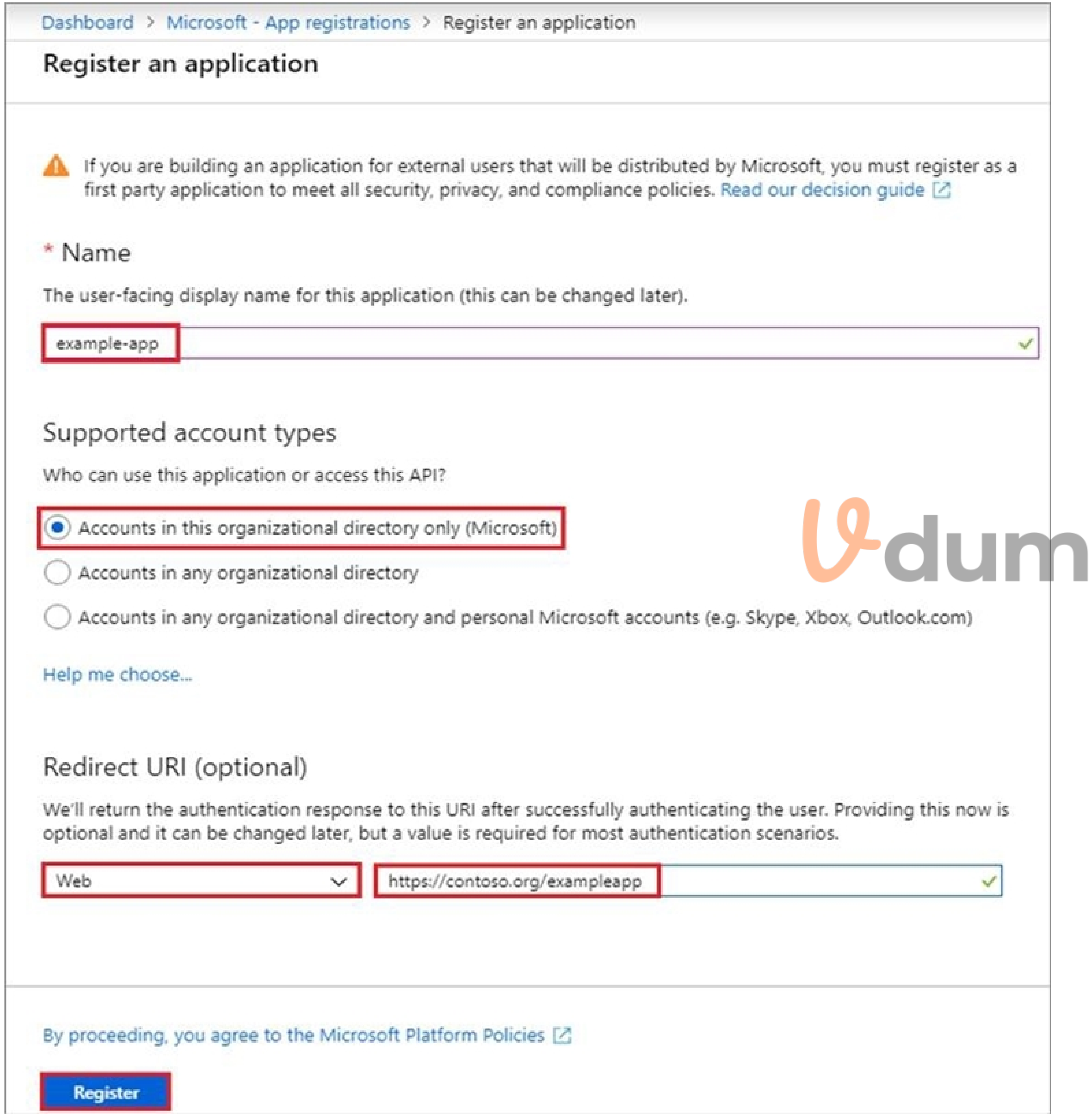
Section:
Explanation:
Box 1; User2
Billing Administrator
Select Transfer billing ownership for the subscription that you want to transfer.
Enter the email address of a user who's a billing administrator of the account that will be the new owner for the subscription.
Box 2: Azure Account Center
Azure Account Center can be used.
Reference:
https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer#transfer-billing-ownership-of-an-azure-subscription

QUESTION 36
SIMULATION
The developers at your company plan to create a web app named App10598168 and to publish the app to https://www.contoso.com.
You need to perform the following tasks:
Ensure that App10598168 is registered to Azure Active Directory (Azure AD).
Generate a password for App10598168.
To complete this task, sign in to the Azure portal.

A.

Correct Answer: A
Section:
Explanation:
Answer: A
Explanation:
Step 1: Register the Application
1. Sign in to your Azure Account through the Azure portal.

2. Select Azure Active Directory.
3. Select App registrations.
4. Select New registration.
5. Name the application App10598168 . Select a supported account type, which determines who can use the application. Under Redirect URI, select Web for the type of application you want to create. Enter the URI: https://www.contoso.com , where the access token is sent to.



Dashboard > Microsoft - App registrations > Register an application

Register an application

If you are building an application for external users that will be distributed by Microsoft, you must register as a first party application to meet all security, privacy, and compliance policies. Read our decision guide

* Name

The user-facing display name for this application (this can be changed later).

example-app ✓

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Microsoft)
○ Accounts in any organizational directory
○ Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web ⌄ https://contoso.org/exampleapp ✓

By proceeding, you agree to the Microsoft Platform Policies

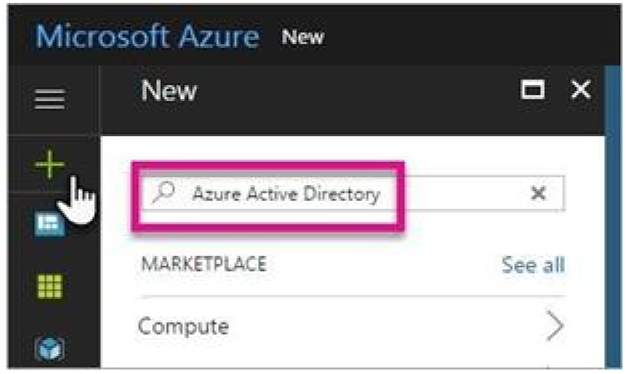
6. Click Register
Step 2: Create a new application secret
If you choose not to use a certificate, you can create a new application secret.
7 Select Certificates & secrets.

8. Select Client secrets -> New client secret.
9. Provide a description of the secret, and a duration. When done, select Add.
After saving the client secret, the value of the client secret is displayed. Copy this value because you aren't able to retrieve the key later. You provide the key value with the application ID to sign in as the application. Store the key value where your application can retrieve it.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal

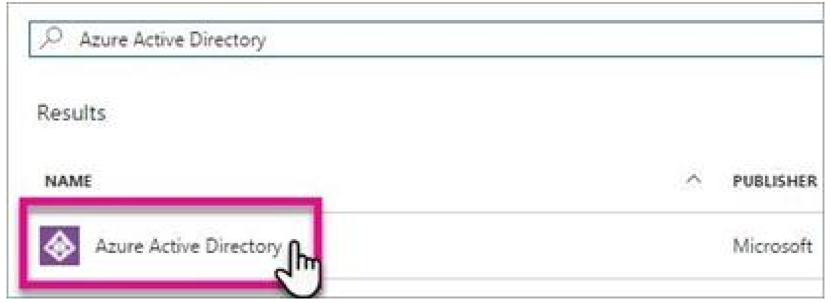
QUESTION 37
SIMULATION
You need to create a new Azure Active Directory (Azure AD) directory named 11641655.onmicrosoft.com and a user named User1 in the new directory. The solution must ensure that User1 is enabled for Azure Multi-Factor Authentication
(MFA).
To complete this task, sign in to the Azure portal.

A.

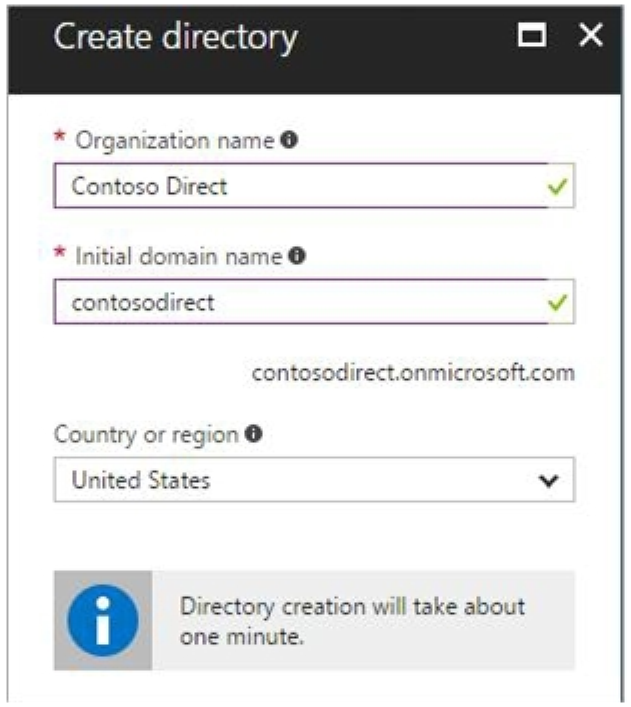
Correct Answer: A
Section:
Explanation:
Answer: A
Explanation:
Step 1: Create an Azure Active Directory tenant
1. Browse to the Azure portal and sign in with an account that has an Azure subscription.
2. Select the plus icon (+) and search for Azure Active Directory.



3. Select Azure Active Directory in the search results.



4. Select Create.
5. Provide an Organization name and an Initial domain name (10598168). Then select Create. Your directory is created.



Create directory

* Organization name: Contoso Direct

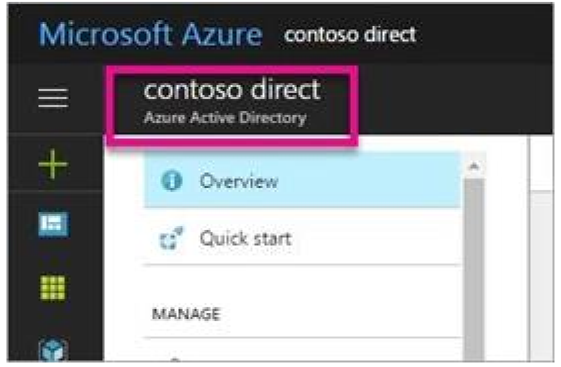
* Initial domain name: contosodirect

contosodirect.onmicrosoft.com

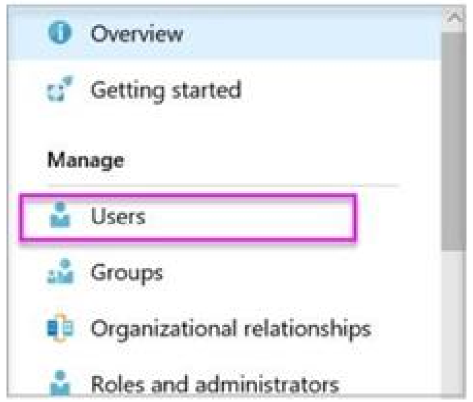
Country or region: United States

Directory creation will take about one minute.

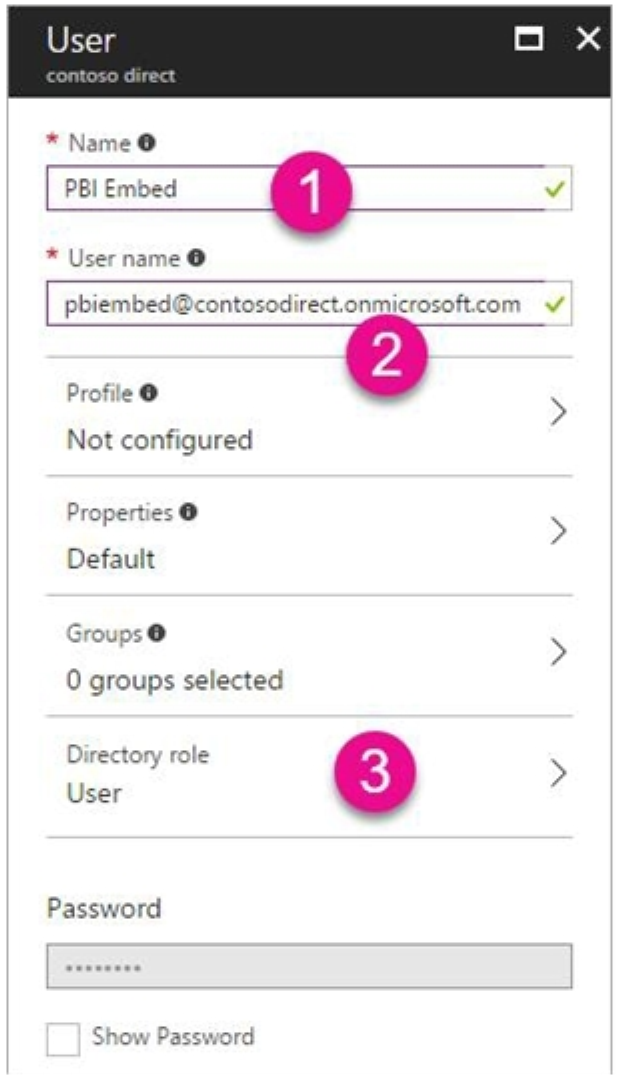
6. After directory creation is complete, select the information box to manage your new directory.
Next, you're going to add tenant users.
Step 2: Create an Azure Active Directory tenant user
7. In the Azure portal, make sure you are on the Azure Active Directory fly out.



8. Under Manage, select Users.



9. Select All users and then select + New user.
10. Provide a Name and User name (user1) for the regular user tenant You can also show the temporary password. When you're done, select Create.
Name: user1
User name: user1@11641655.onmicrosoft.com



User

contoso direct

* Name: PBI Embed ✓

* User name: pbiembed@contosodirect.onmicrosoft.com ✓

Profile: Not configured

Properties: Default

Groups: 0 groups selected

Directory role: User

Password: ••••••••

□ Show Password

Reference:
https://docs.microsoft.com/en-us/power-bi/developer/create-an-azure-active-directory-tenant

QUESTION 38

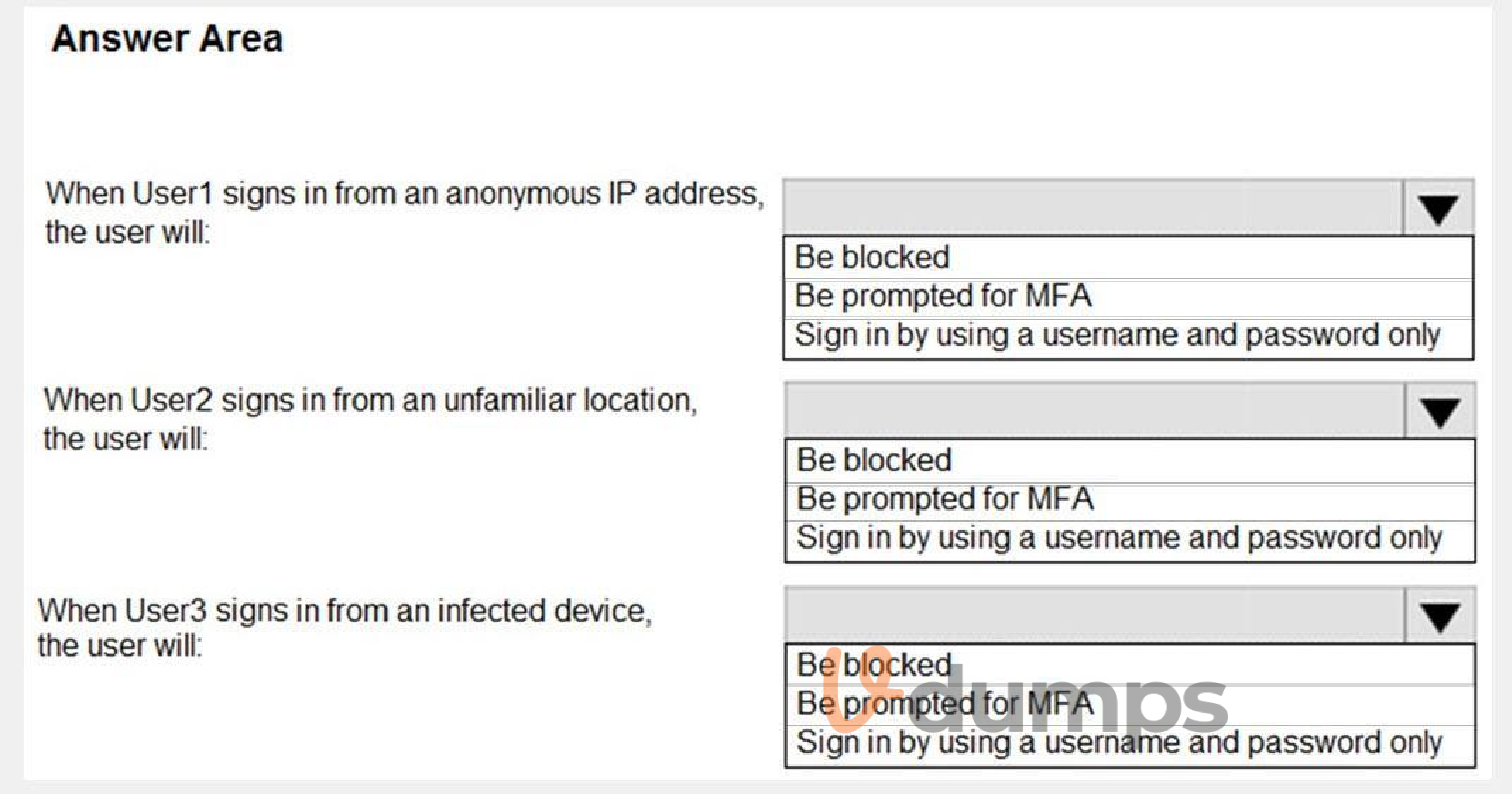
HOTSPOT

You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

Name	Member of	Multi-factor authentication (MFA) status
User1	Group1, Group2	Enabled
User2	Group1	Disabled
User3	Group1	Disabled

You create and enforce an Azure AD Identity Protection sign-in risk policy that has the following settings:
Assignments: Include Group1, exclude Group2
Conditions: Sign-in risk level: Medium and above
Access Allow access, Require multi-factor authentication
You need to identify what occurs when the users sign in to Azure AD.
What should you identify for each user? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

When User1 signs in from an anonymous IP address, the user will:

- Be blocked
- Be prompted for MFA
- Sign in by using a username and password only

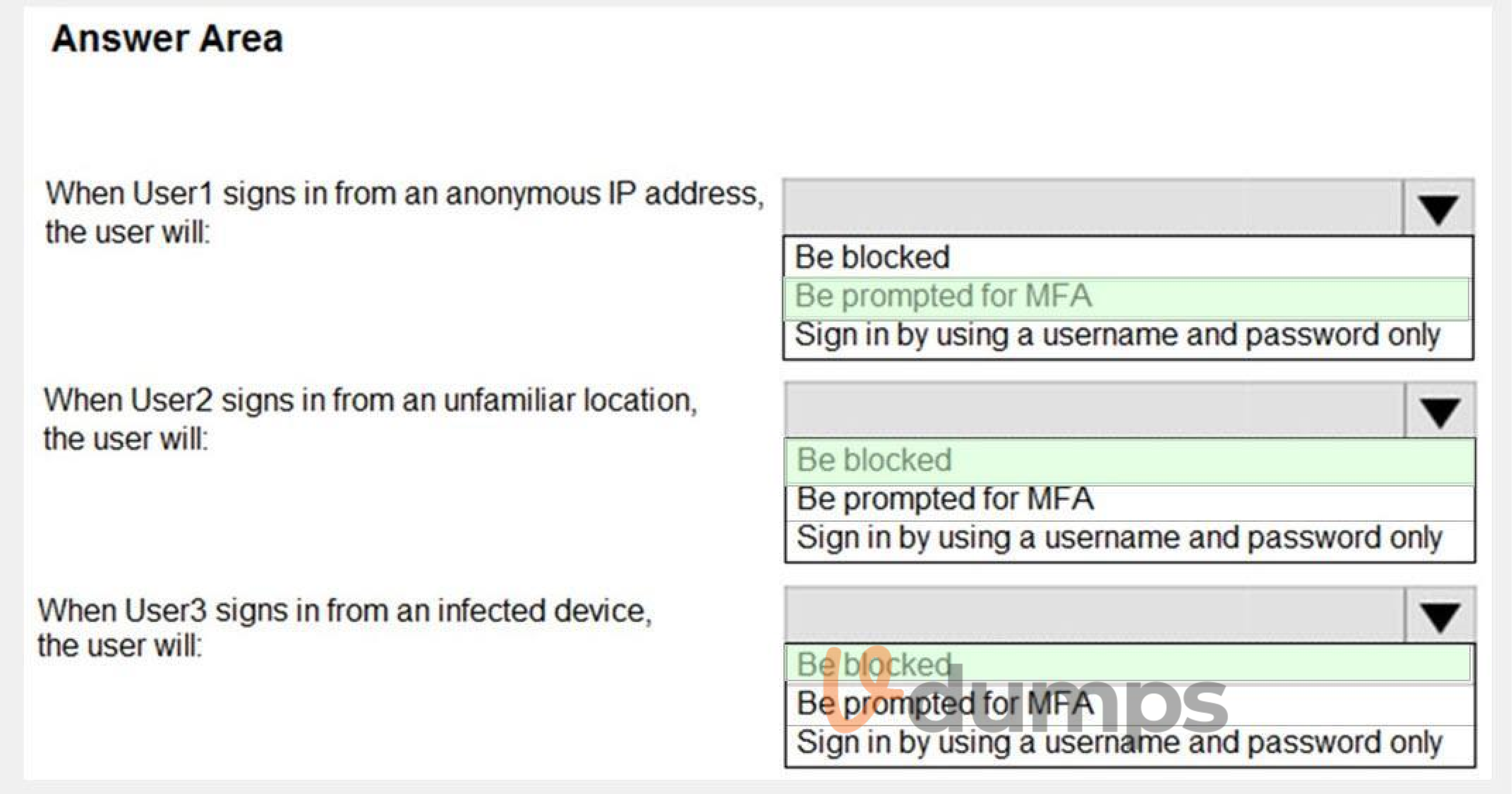
When User2 signs in from an unfamiliar location, the user will:

- Be blocked
- Be prompted for MFA
- Sign in by using a username and password only

When User3 signs in from an infected device, the user will:

- Be blocked
- Be prompted for MFA
- Sign in by using a username and password only

Answer Area:



Answer Area

When User1 signs in from an anonymous IP address, the user will:

- Be blocked
- [✓ Be prompted for MFA]
- Sign in by using a username and password only

When User2 signs in from an unfamiliar location, the user will:

- [✓ Be blocked]
- Be prompted for MFA
- Sign in by using a username and password only

When User3 signs in from an infected device, the user will:

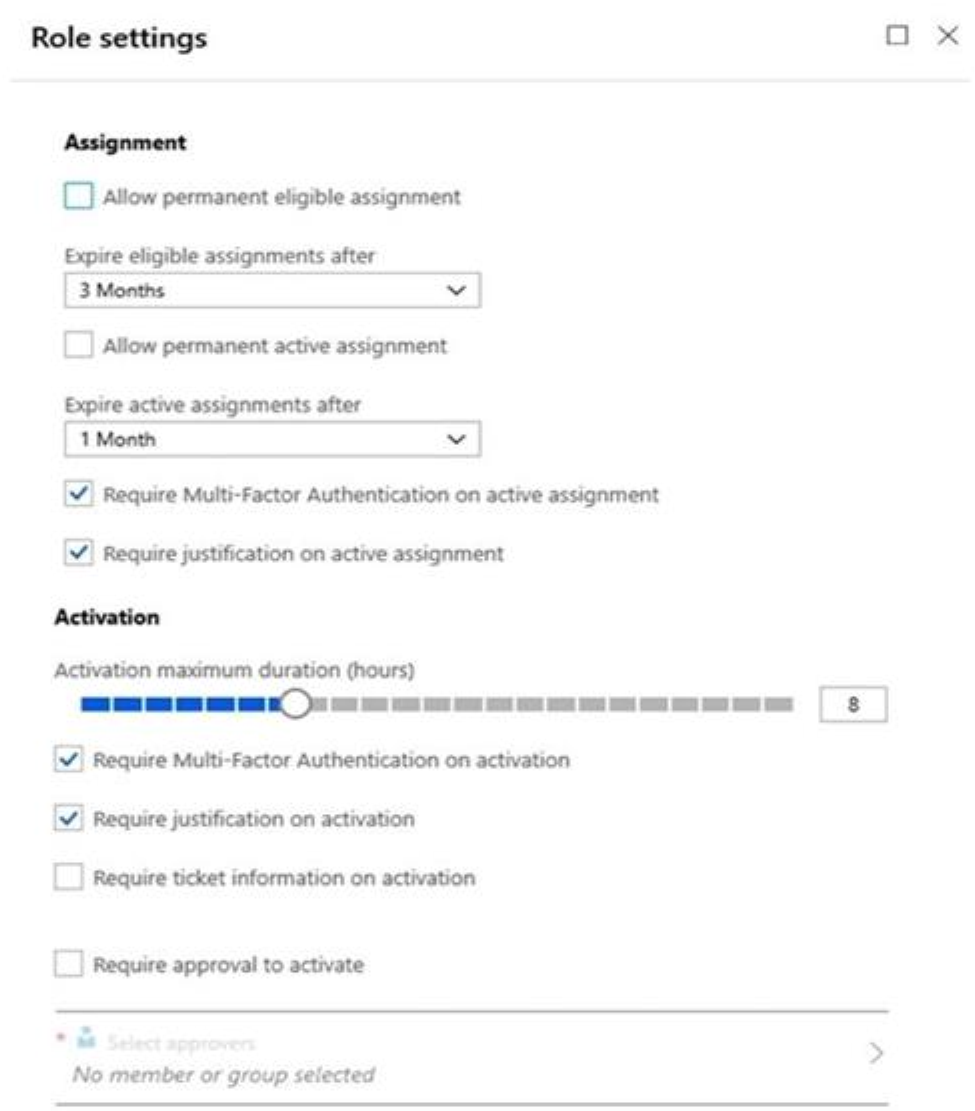
- [✓ Be blocked]
- Be prompted for MFA
- Sign in by using a username and password only

Section:
Explanation:
References:
http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks

QUESTION 39
HOTSPOT
You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

Name	Multi-factor authentication (MFA) status
User1	Disabled
User2	Disabled
User3	Enforced

In Azure AD Privileged Identity Management (PIM), the Role settings for the Contributor role are configured as shown in the exhibit. (Click the Exhibit tab.)



Role settings

Assignment

□ Allow permanent eligible assignment

Expire eligible assignments after

3 Months

□ Allow permanent active assignment

Expire active assignments after

1 Month

☑ Require Multi-Factor Authentication on active assignment

☑ Require justification on active assignment

Activation

Activation maximum duration (hours)

8

☑ Require Multi-Factor Authentication on activation

☑ Require justification on activation

□ Require ticket information on activation

□ Require approval to activate

* Select approvers

No member or group selected

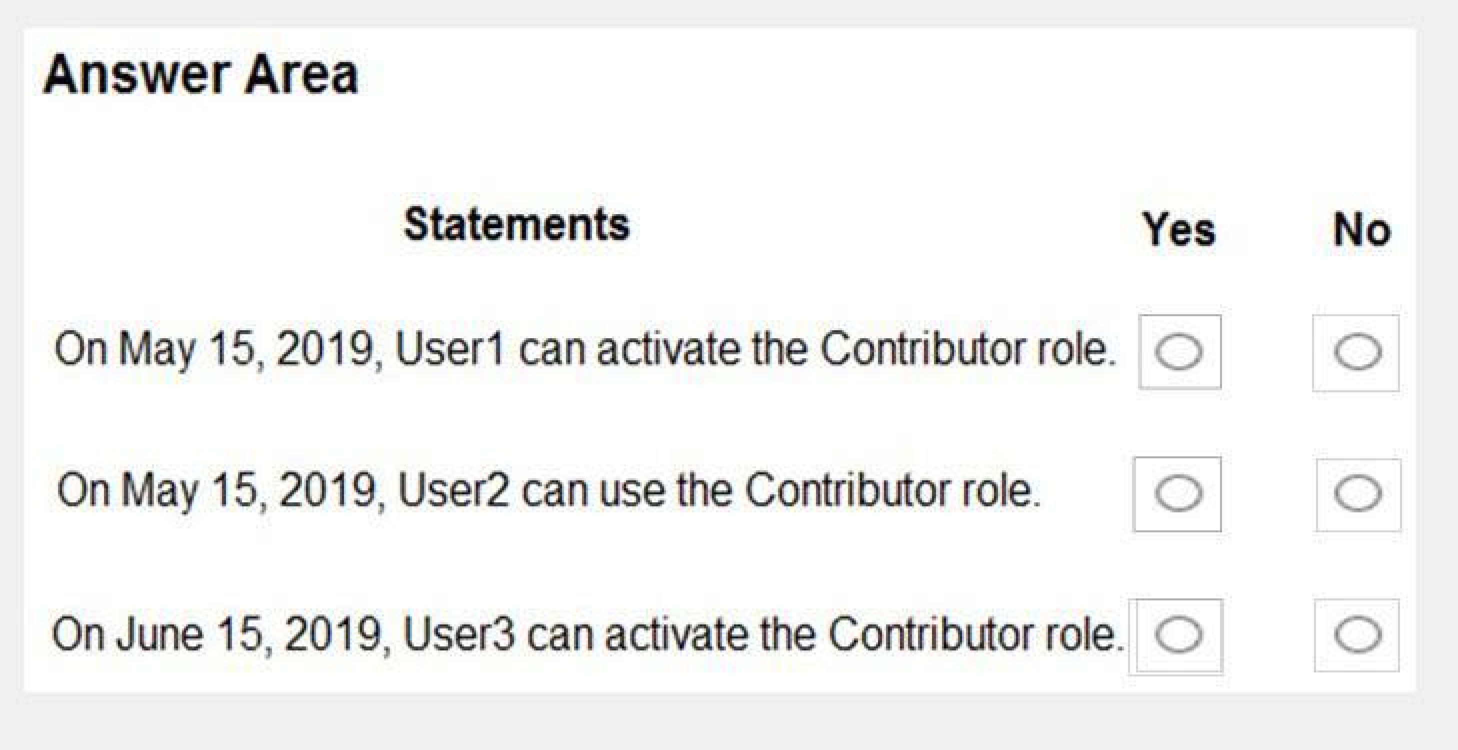
You assign users the Contributor role on May 1, 2019 as shown in the following table.

Name	Assignment type
User1	Eligible
User2	Active
User3	Active

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

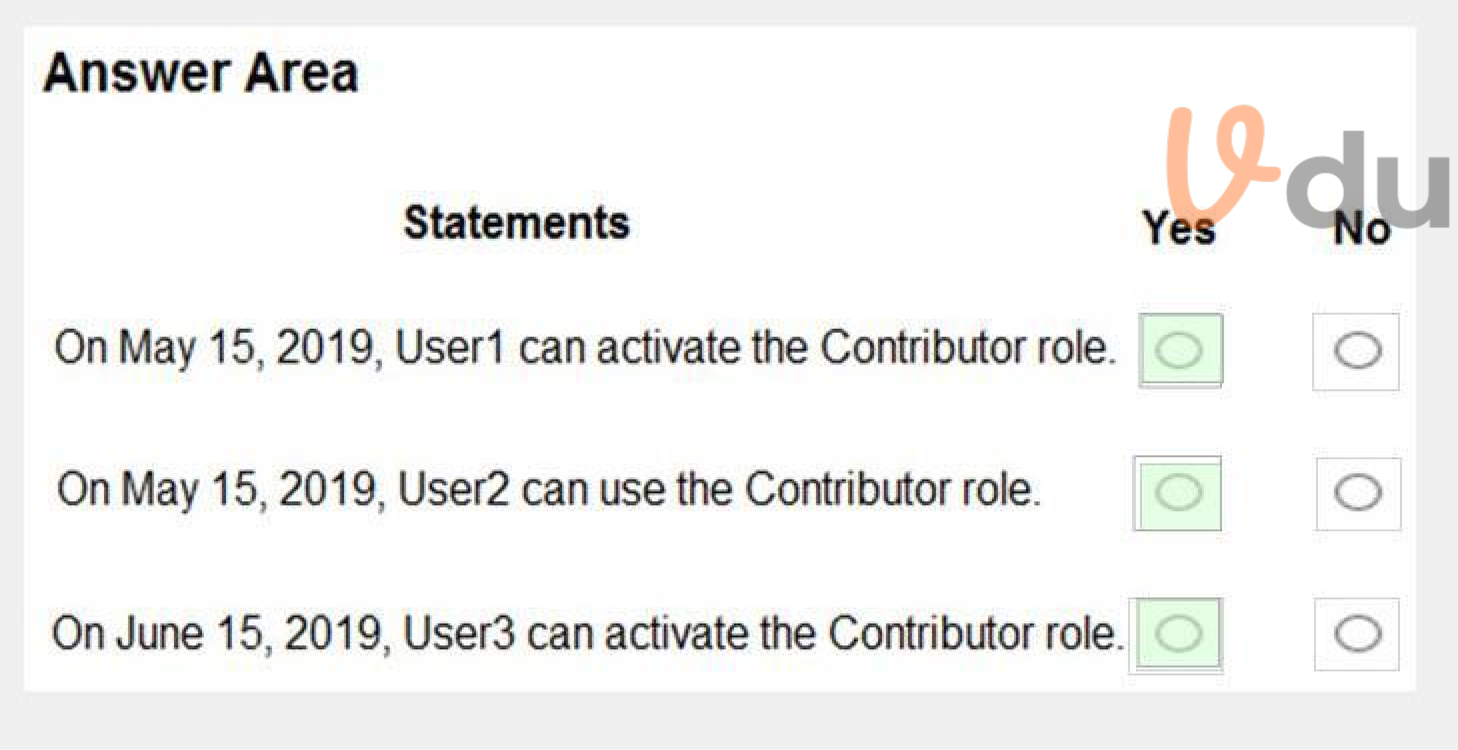
Hot Area:



Answer Area

Statements	Yes	No
On May 15, 2019, User1 can activate the Contributor role.	○	○
On May 15, 2019, User2 can use the Contributor role.	○	○
On June 15, 2019, User3 can activate the Contributor role.	○	○

Answer Area:

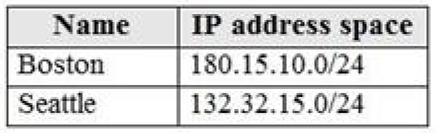


Answer Area

Statements	Yes	No
On May 15, 2019, User1 can activate the Contributor role.	[✓ ○]	○
On May 15, 2019, User2 can use the Contributor role.	[✓ ○]	○
On June 15, 2019, User3 can activate the Contributor role.	[✓ ○]	○

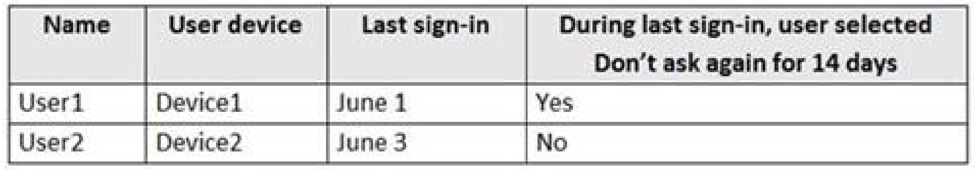
Section:
Explanation:
References:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-resource-roles-assign-roles

QUESTION 40
HOTSPOT
You work at a company named Contoso, Ltd. that has the offices shown in the following table.



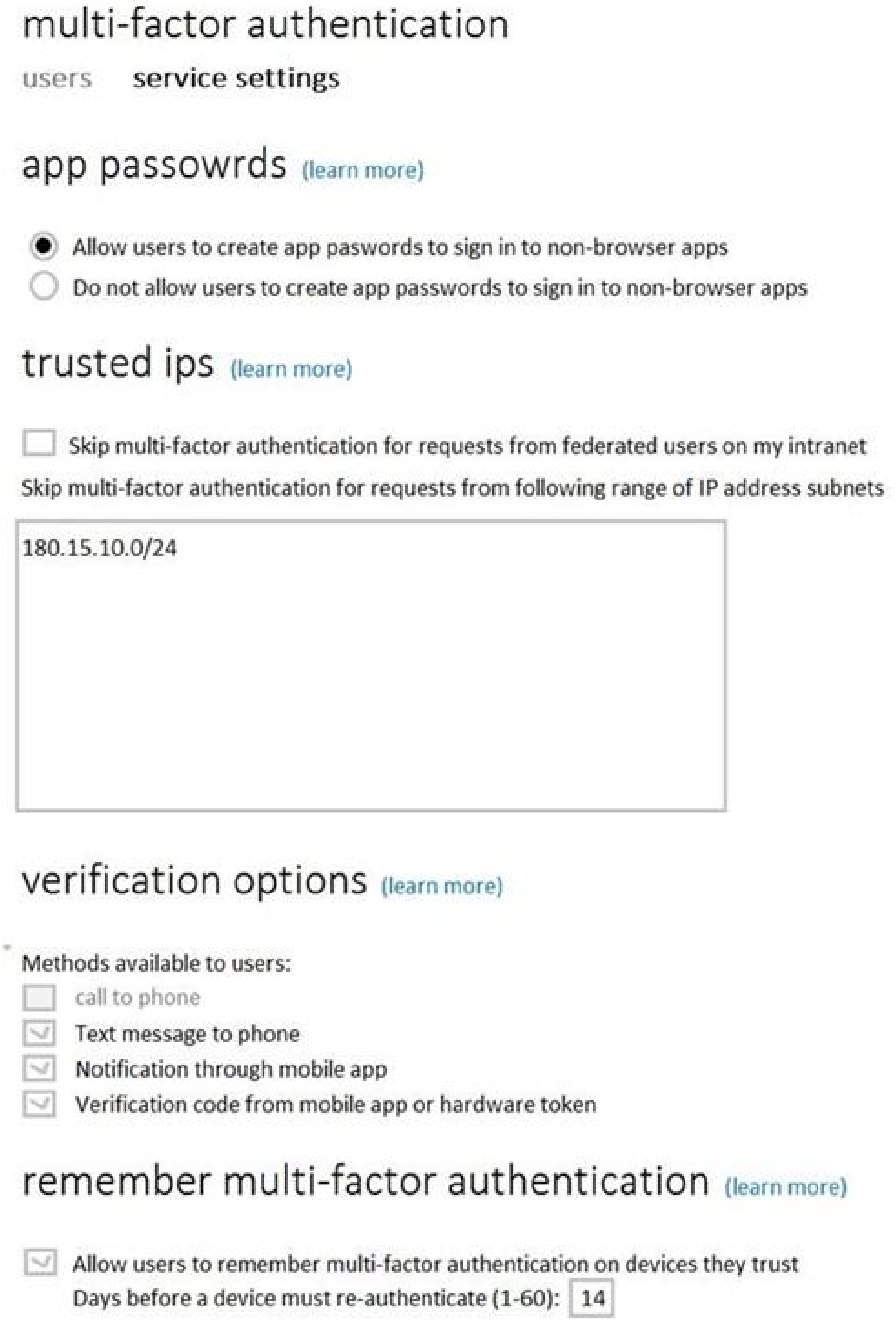
Name	IP address space
Boston	180.15.10.0/24
Seattle	132.32.15.0/24

Contoso has an Azure Active Directory (Azure AD) tenant named contoso.com. All contoso.com users have Azure Multi-Factor Authentication (MFA) enabled. The tenant contains the users shown in the following table.



Name	User device	Last sign-in	During last sign-in, user selected Don't ask again for 14 days
User1	Device1	June 1	Yes
User2	Device2	June 3	No

The multi-factor settings for contoso.com are configured as shown in the following exhibit.



multi-factor authentication

users service settings

app passowrds (learn more)

● Allow users to create app paswords to sign in to non-browser apps
○ Do not allow users to create app passwords to sign in to non-browser apps

trusted ips (learn more)

□ Skip multi-factor authentication for requests from federated users on my intranet

Skip multi-factor authentication for requests from following range of IP address subnets

180.15.10.0/24

verification options (learn more)

Methods available to users:

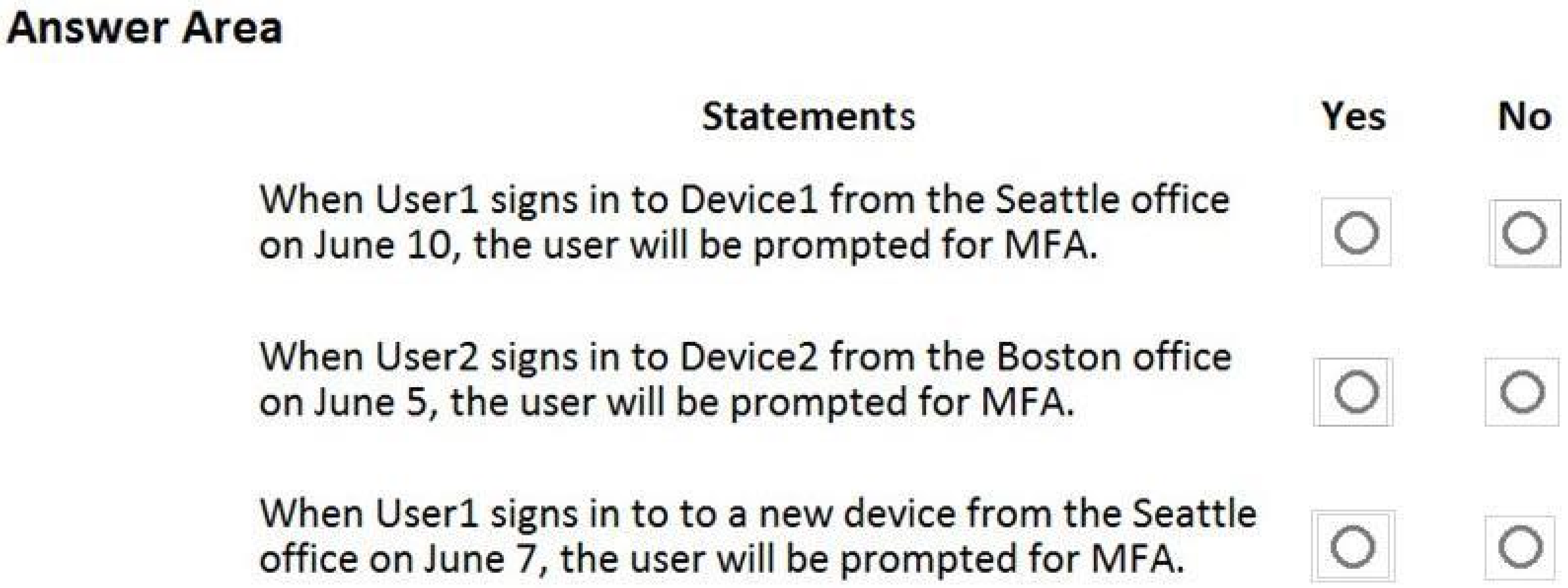
□ call to phone
☑ Text message to phone
☑ Notification through mobile app
☑ Verification code from mobile app or hardware token

remember multi-factor authentication (learn more)

☑ Allow users to remember multi-factor authentication on devices they trust
Days before a device must re-authenticate (1-60): 14

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

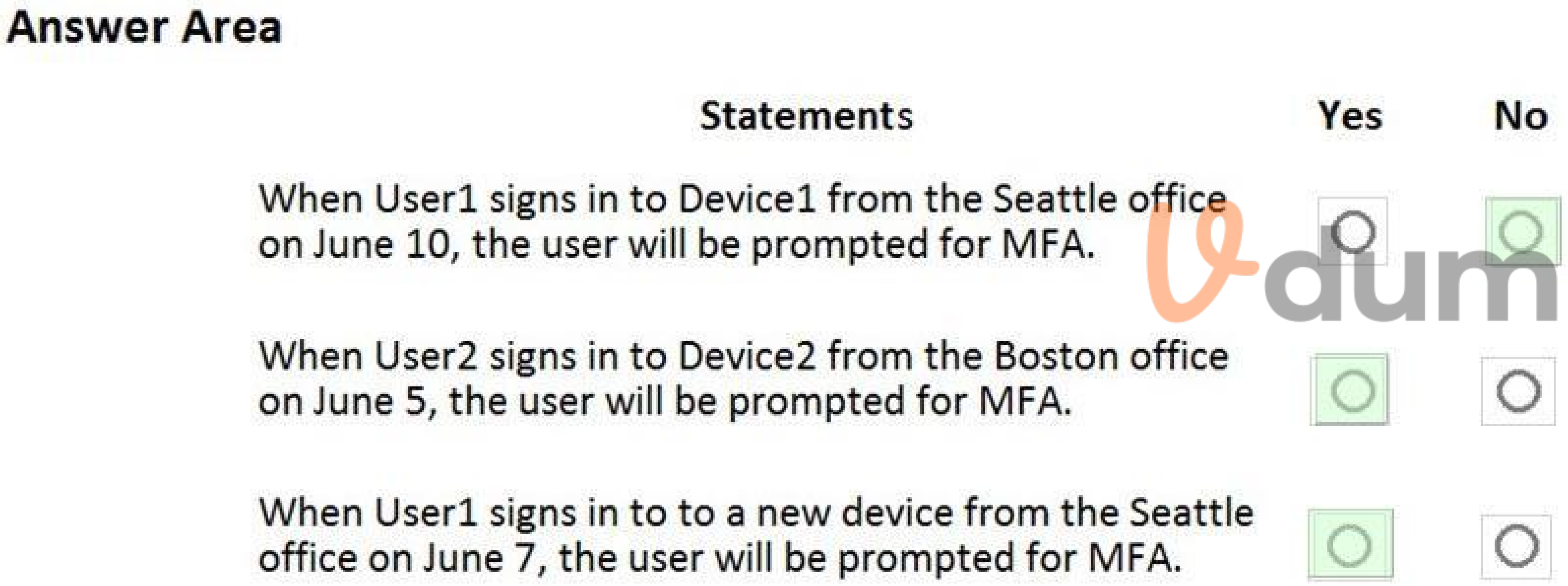
Hot Area:



Answer Area

Statements	Yes	No
When User1 signs in to Device1 from the Seattle office on June 10, the user will be prompted for MFA.	○	○
When User2 signs in to Device2 from the Boston office on June 5, the user will be prompted for MFA.	○	○
When User1 signs in to to a new device from the Seattle office on June 7, the user will be prompted for MFA.	○	○

Answer Area:



Answer Area

Statements	Yes	No
When User1 signs in to Device1 from the Seattle office on June 10, the user will be prompted for MFA.	○	[✓ ○]
When User2 signs in to Device2 from the Boston office on June 5, the user will be prompted for MFA.	[✓ ○]	○
When User1 signs in to to a new device from the Seattle office on June 7, the user will be prompted for MFA.	[✓ ○]	○

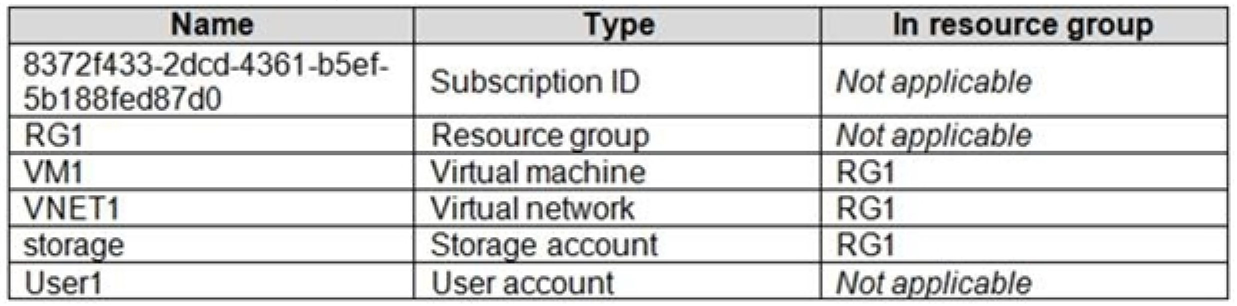
Section:

Explanation:

QUESTION 41

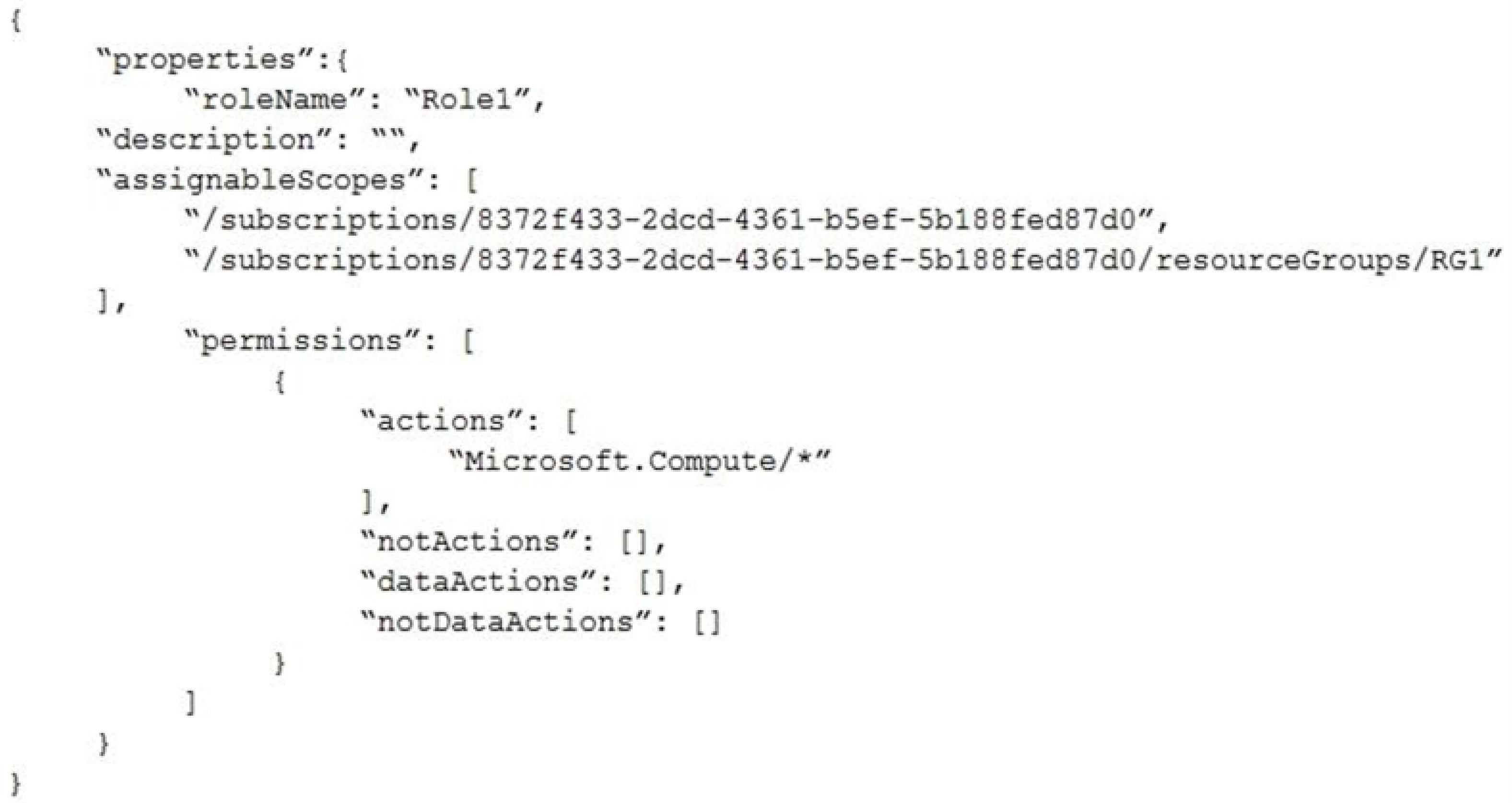
HOTSPOT

You have an Azure subscription named Subscription1 that contains the resources shown in the following table.



Name	Type	In resource group
8372f433-2dcd-4361-b5ef-5b188fed87d0	Subscription ID	*Not applicable*
RG1	Resource group	*Not applicable*
VM1	Virtual machine	RG1
VNET1	Virtual network	RG1
storage	Storage account	RG1
User1	User account	*Not applicable*

You create an Azure role by using the following JSON file.



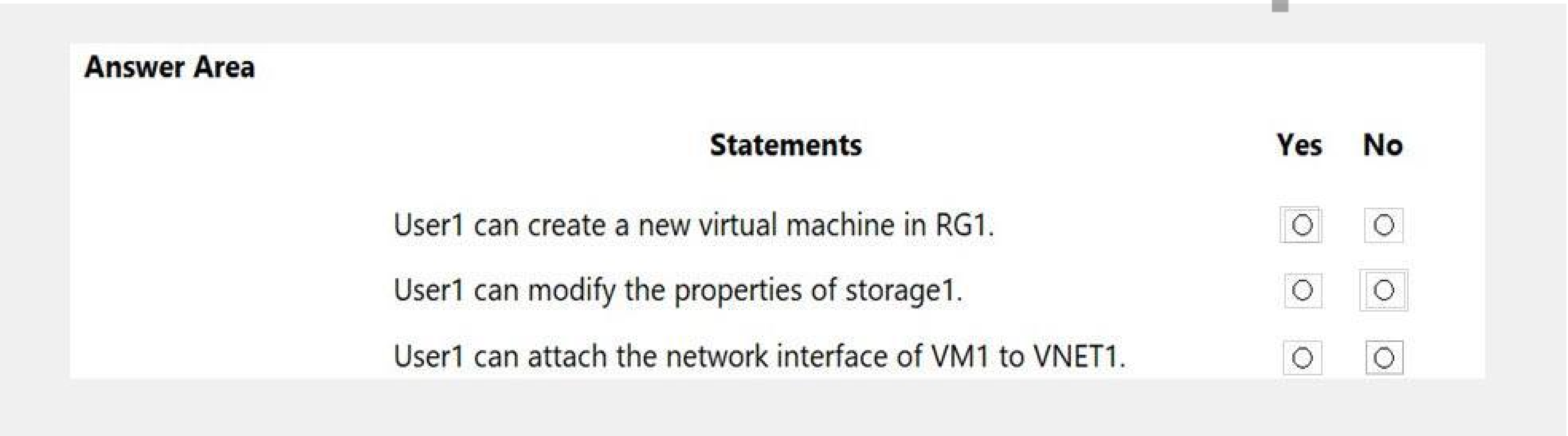
```
{
      “properties”:{
            “roleName”: “Role1”,
      “description”: “”,
      “assignableScopes”: [
            “/subscriptions/8372f433-2dcd-4361-b5ef-5b188fed87d0”,
            “/subscriptions/8372f433-2dcd-4361-b5ef-5b188fed87d0/resourceGroups/RG1”
      ],
            “permissions”: [
                  {
                        “actions”: [
                              “Microsoft.Compute/*”
                        ],
                        “notActions”: [],
                        “dataActions”: [],
                        “notDataActions”: []
                  }
            ]
      }
}
```

You assign Role1 to User1 for RG1.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

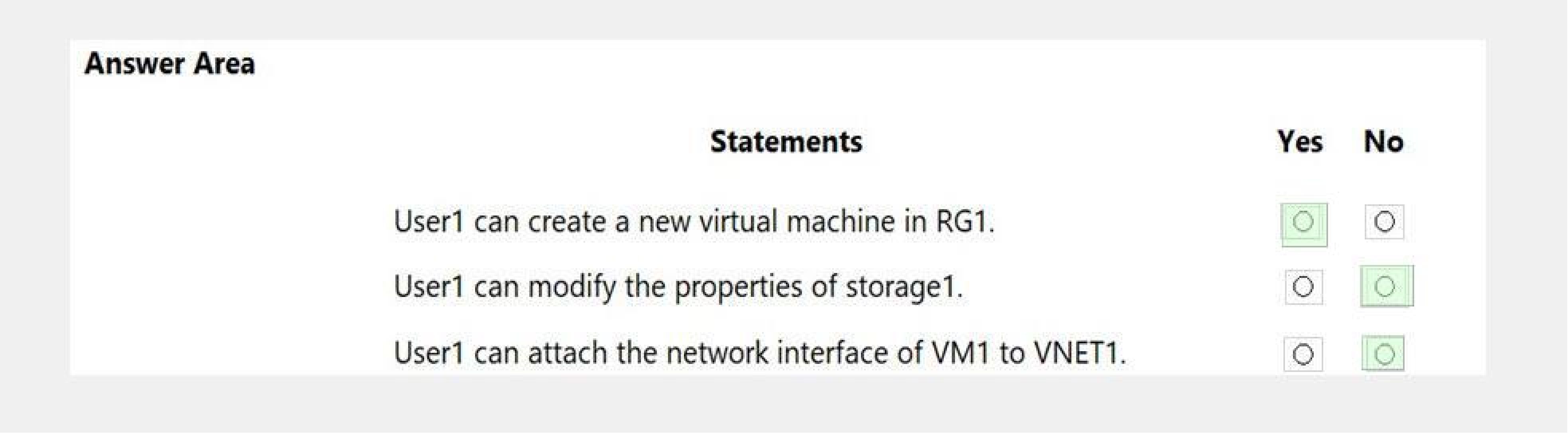
Hot Area:



Answer Area

Statements	Yes	No
User1 can create a new virtual machine in RG1.	○	○
User1 can modify the properties of storage1.	○	○
User1 can attach the network interface of VM1 to VNET1.	○	○

Answer Area:



Answer Area

Statements	Yes	No
User1 can create a new virtual machine in RG1.	[✓ ○]	○
User1 can modify the properties of storage1.	○	[✓ ○]
User1 can attach the network interface of VM1 to VNET1.	○	[✓ ○]

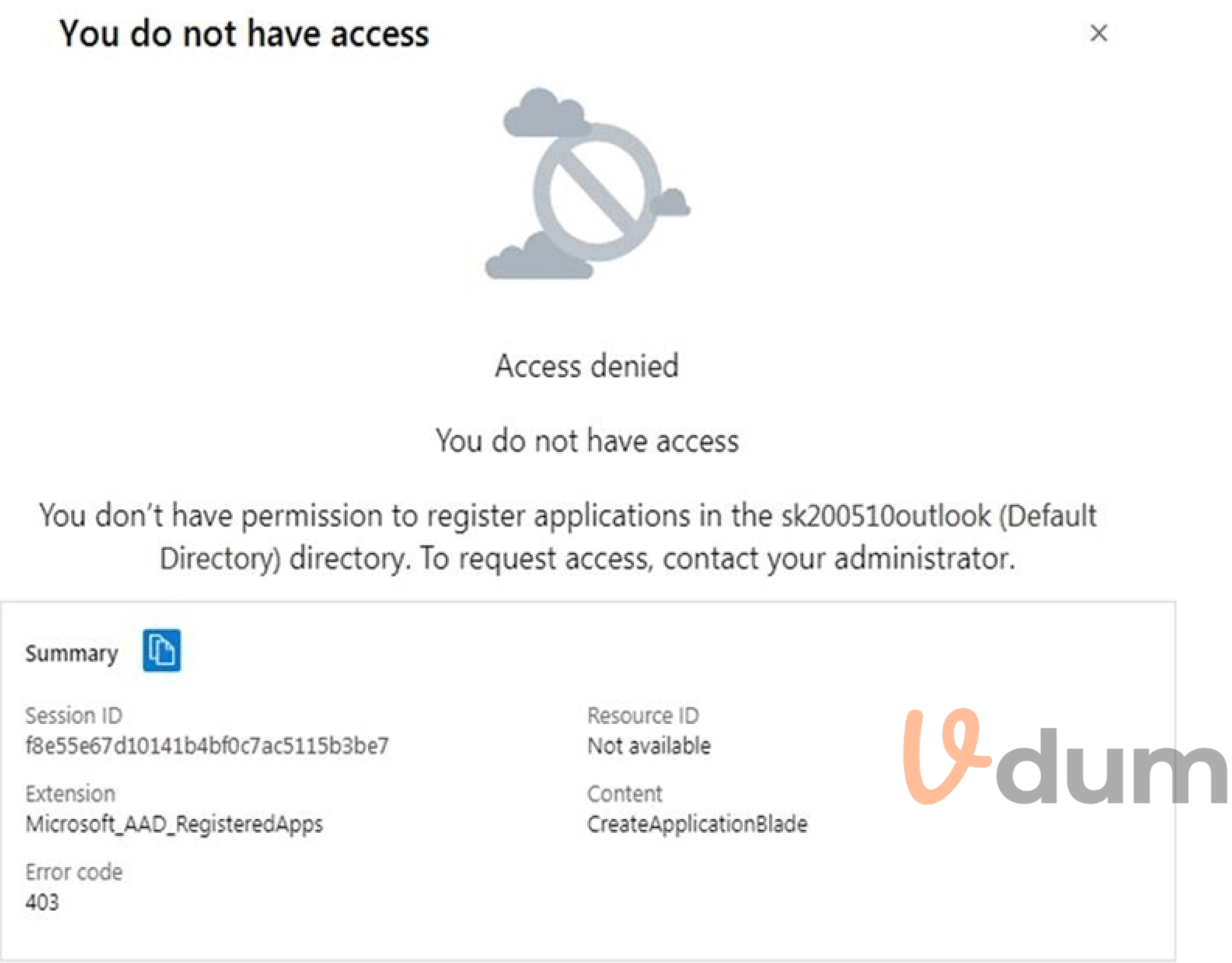
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#compute

QUESTION 42
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains a user named User1.
You plan to publish several apps in the tenant.
You need to ensure that User1 can grant admin consent for the published apps.
Which two possible user roles can you assign to User1 to achieve this goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Security administrator
B. Cloud application administrator
C. Application administrator
D. User administrator
E. Application developer

Correct Answer: B, C
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent

QUESTION 43
You have an Azure subscription that is associated with an Azure Active Directory (Azure AD) tenant.
When a developer attempts to register an app named App1 in the tenant, the developer receives the error message shown in the following exhibit.



You do not have access

Access denied

You do not have access

You don't have permission to register applications in the sk200510outlook (Default Directory) directory. To request access, contact your administrator.

Summary

Session ID
f8e55e67d10141b4bf0c7ac5115b3be7

Resource ID
Not available

Extension
Microsoft_AAD_RegisteredApps

Content
CreateApplicationBlade

Error code
403

You need to ensure that the developer can register App1 in the tenant.
What should you do for the tenant?

A. Modify the Directory properties.

B. Set Enable Security defaults to Yes.

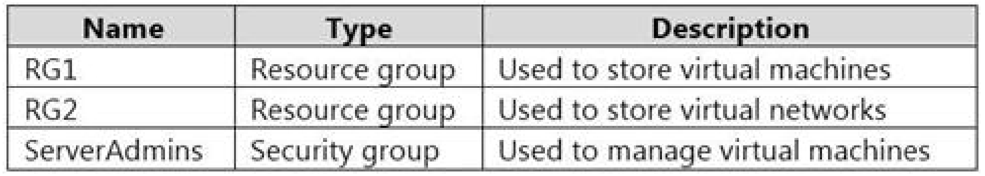
C. Configure the Consent and permissions settings for enterprise applications.

D. Modify the User settings.

Correct Answer: D
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added

QUESTION 44

You have an Azure subscription that contains the resources shown in the following table.



Name	Type	Description
RG1	Resource group	Used to store virtual machines
RG2	Resource group	Used to store virtual networks
ServerAdmins	Security group	Used to manage virtual machines

You need to ensure that ServerAdmins can perform the following tasks:

Create virtual machines in RG1 only.

Connect the virtual machines to the existing virtual networks in RG2 only.

The solution must use the principle of least privilege.

Which two role-based access control (RBAC) roles should you assign to ServerAdmins? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. a custom RBAC role for RG2

B. the Network Contributor role for RG2

C. the Contributor role for the subscription

D. a custom RBAC role for the subscription

E. the Network Contributor role for RG1

F. the Virtual Machine Contributor role for RG1

Correct Answer: A, F

Section:

Explanation:

Reference:

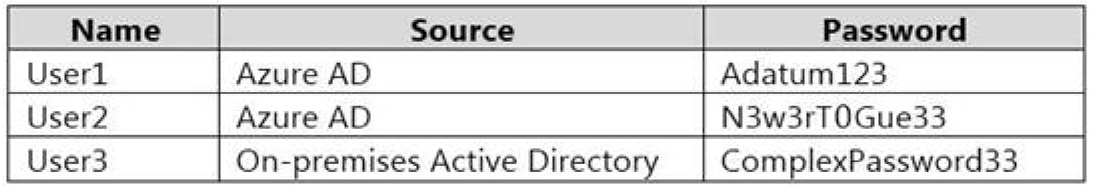
https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

QUESTION 45

HOTSPOT

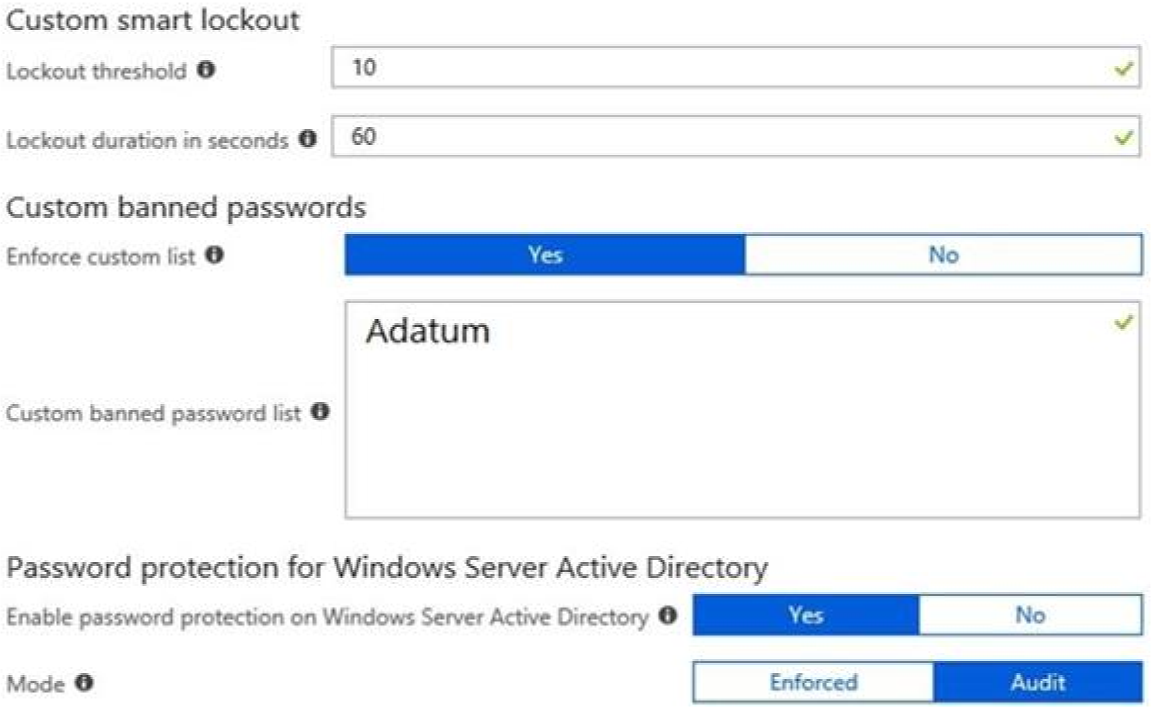
Your network contains an on-premises Active Directory domain named adatum.com that syncs to Azure Active Directory (Azure AD).

The Azure AD tenant contains the users shown in the following table.



Name	Source	Password
User1	Azure AD	Adatum123
User2	Azure AD	N3w3rT0Gue33
User3	On-premises Active Directory	ComplexPassword33

You configure the Authentication methods – Password Protection settings for adatum.com as shown in the following exhibit.



Custom smart lockout

Lockout threshold	10 ✓
Lockout duration in seconds	60 ✓

Custom banned passwords

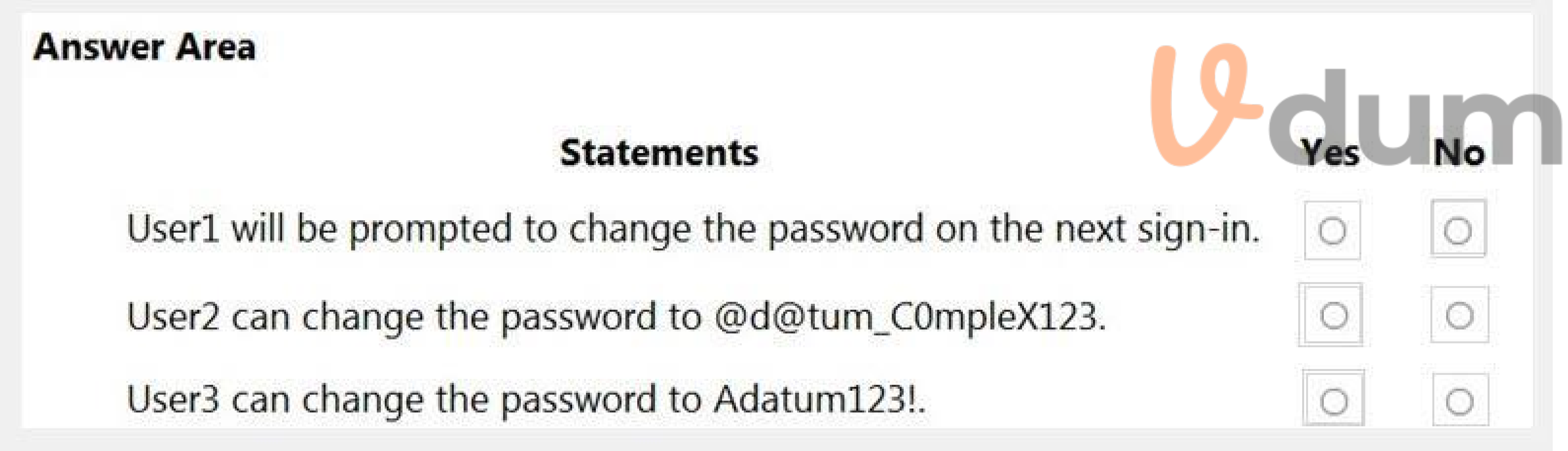
Enforce custom list	[✓ Yes] No
Custom banned password list	Adatum ✓

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory	[✓ Yes] No
Mode	Enforced [✓ Audit]

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

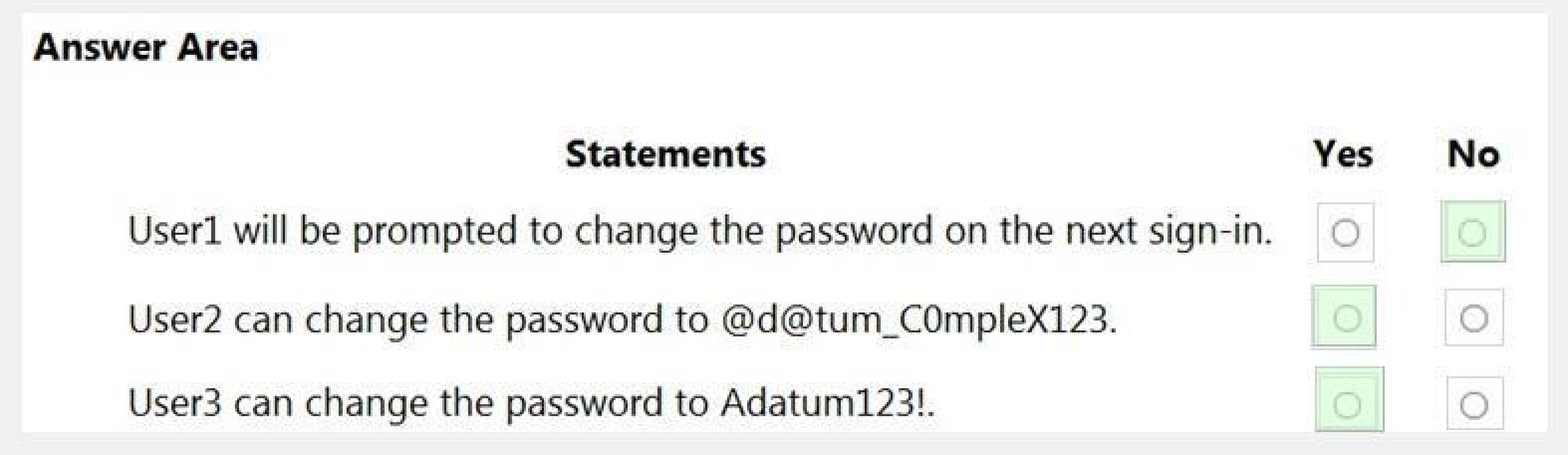
Hot Area:



Answer Area

Statements	Yes	No
User1 will be prompted to change the password on the next sign-in.	○	○
User2 can change the password to @d@tum_C0mpleX123.	○	○
User3 can change the password to Adatum123!.	○	○

Answer Area:



Answer Area

Statements	Yes	No
User1 will be prompted to change the password on the next sign-in.	○	[✓ ○]
User2 can change the password to @d@tum_C0mpleX123.	[✓ ○]	○
User3 can change the password to Adatum123!.	[✓ ○]	○

Section:
Explanation:
Reference:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-deploy
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad

QUESTION 46

HOTSPOT

Your company has an Azure subscription named Subscription1. Subscription1 is associated with the Azure Active Directory tenant that includes the users shown in the following table.

Name	Role
User1	Global administrator
User2	Billing administrator
User3	Owner
User4	Account Admin

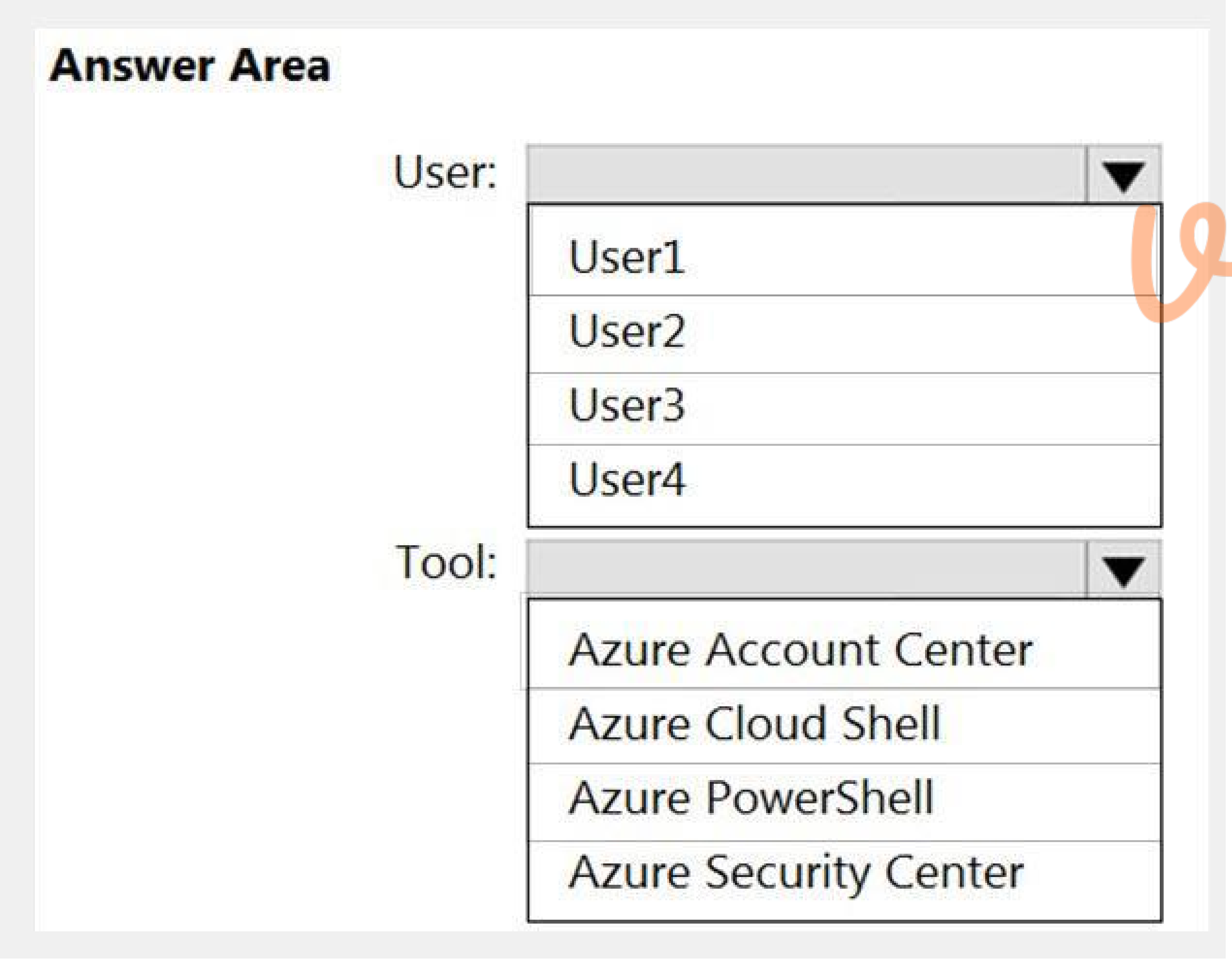
The company is sold to a new owner.

The company needs to transfer ownership of Subscription1.

Which user can transfer the ownership and which tool should the user use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

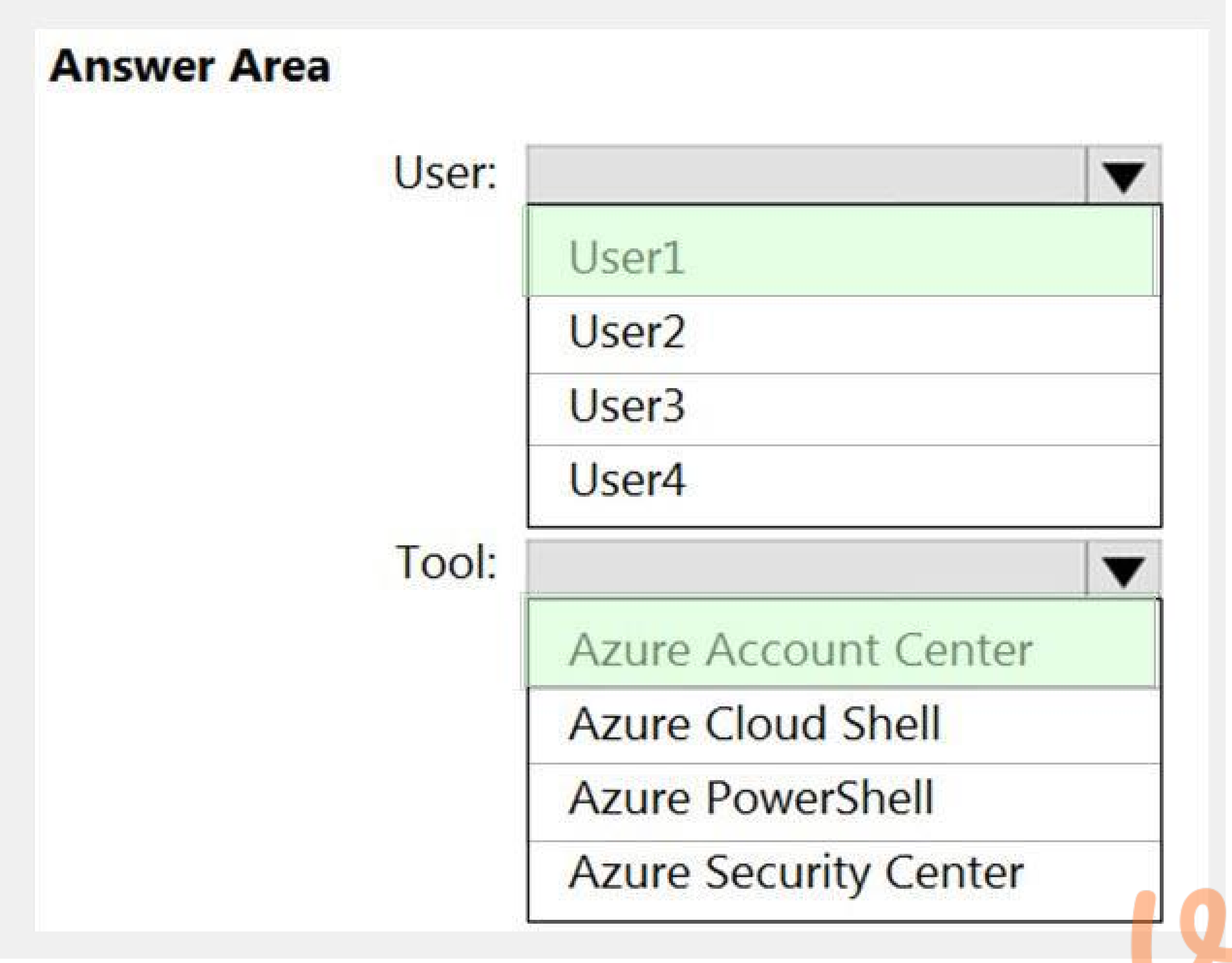


Answer Area

User:

Tool:

Answer Area:



Answer Area

User:

- User1
- User2
- User3
- User4

Tool:

- Azure Account Center
- Azure Cloud Shell
- Azure PowerShell
- Azure Security Center

Section:

Explanation:

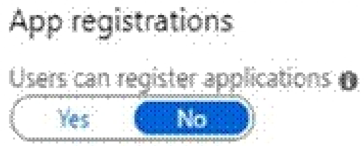
Reference:

https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/billing-subscription-transfer

QUESTION 47

You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant and a user named User1.

The App registrations settings for the tenant are configured as shown in the following exhibit.



App registrations

Users can register applications

Yes [✓ No]

You plan to deploy an app named App1.

You need to ensure that User1 can register App1 in Azure AD. The solution must use the principle of least privilege.

Which role should you assign to User1?

A. App Configuration Data Owner for the subscription

B. Managed Application Contributor for the subscription

C. Cloud application administrator in Azure AD

D. Application developer in Azure AD

Correct Answer: D

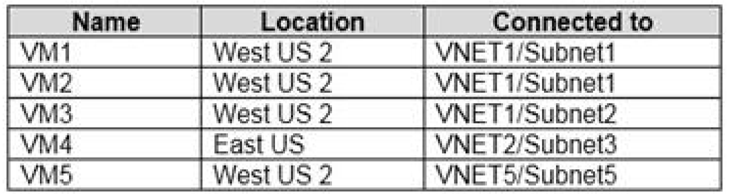
Section:

Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task

QUESTION 48

You have the Azure virtual machines shown in the following table.



Name	Location	Connected to
VM1	West US 2	VNET1/Subnet1
VM2	West US 2	VNET1/Subnet1
VM3	West US 2	VNET1/Subnet2
VM4	East US	VNET2/Subnet3
VM5	West US 2	VNET5/Subnet5

Each virtual machine has a single network interface.
You add the network interface of VM1 to an application security group named ASG1.
You need to identify the network interfaces of which virtual machines you can add to ASG1.
What should you identify?

A. VM2 only

B. VM2 and VM3 only

C. VM2, VM3, VM4, and VM5

D. VM2, VM3, and VM5 only

Correct Answer: B
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/application-security-groups

QUESTION 49

You have an Azure subscription linked to an Azure Active Directory Premium Plan 1 tenant.
You plan to implement Azure Active Directory (Azure AD) Identity Protection.
You need to ensure that you can configure a user risk policy and a sign-in risk policy.
What should you do first?

A. Purchase Azure Active Directory Premium Plan 2 licenses for all users.

B. Register all users for Azure Multi-Factor Authentication (MFA).

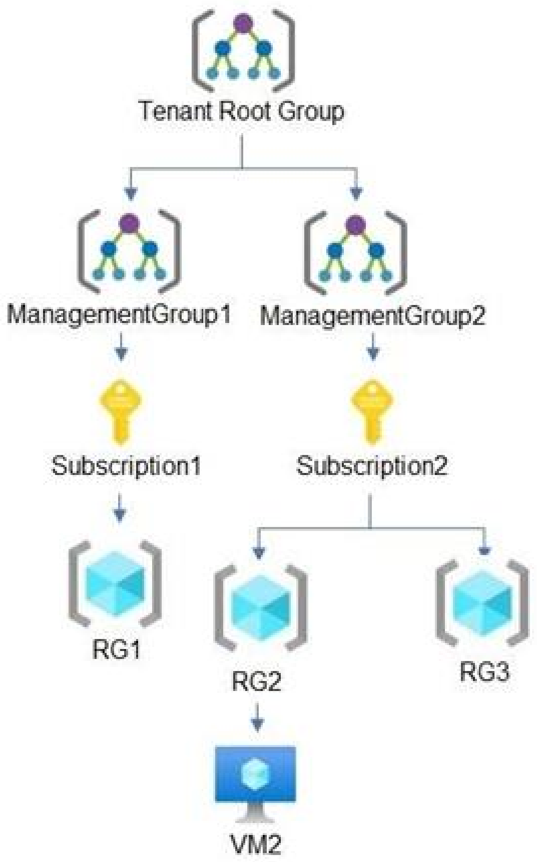
C. Enable security defaults for Azure AD.

D. Enable Azure Defender in Azure Security Center.

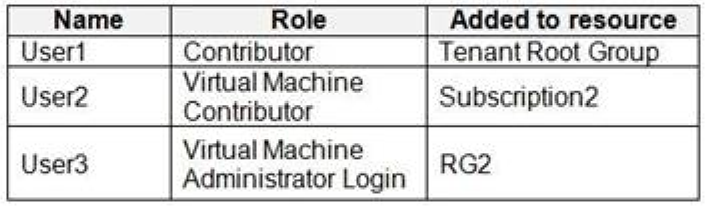
Correct Answer: A
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-risk-based-sspr-mfa

QUESTION 50

HOTSPOT
You have the hierarchy of Azure resources shown in the following exhibit.



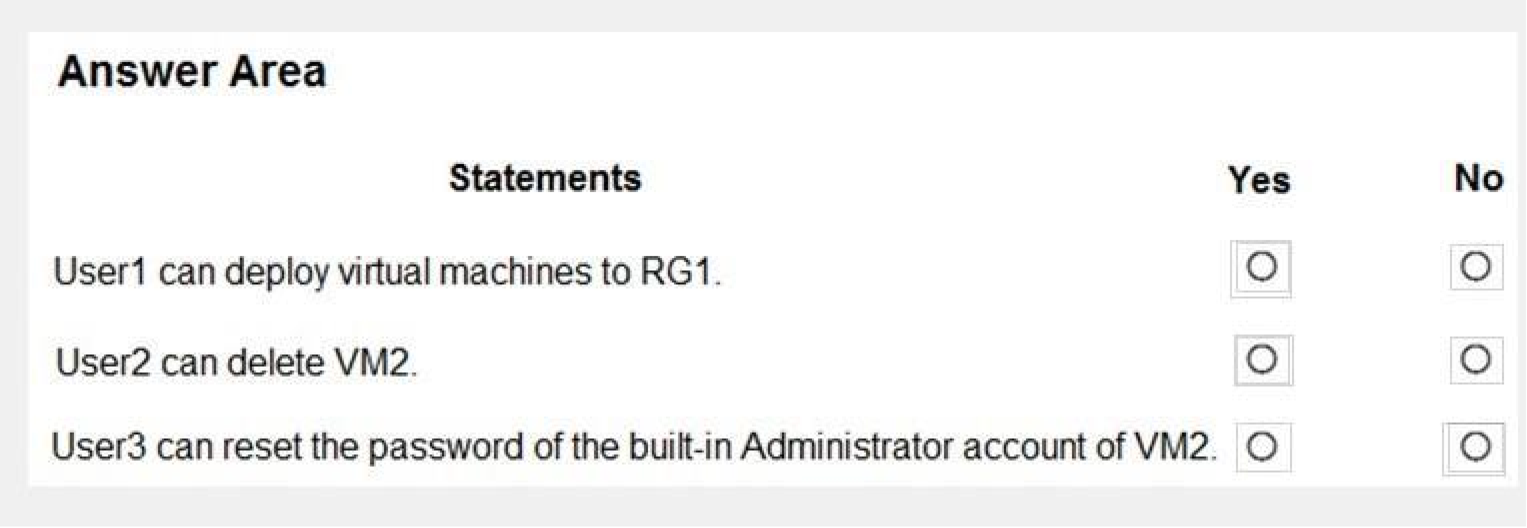
RG1, RG2, and RG3 are resource groups.
RG2 contains a virtual machine named VM1.
You assign role-based access control (RBAC) roles to the users shown in the following table.



Name	Role	Added to resource
User1	Contributor	Tenant Root Group
User2	Virtual Machine Contributor	Subscription2
User3	Virtual Machine Administrator Login	RG2

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

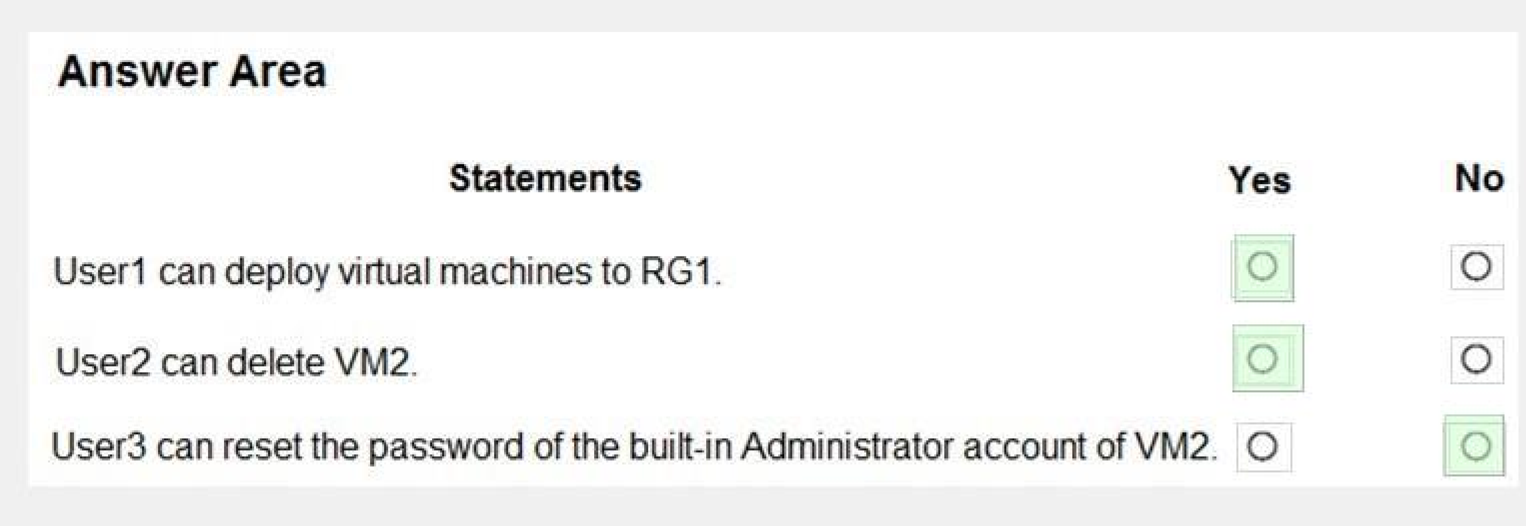
Hot Area:



Answer Area

Statements	Yes	No
User1 can deploy virtual machines to RG1.	○	○
User2 can delete VM2.	○	○
User3 can reset the password of the built-in Administrator account of VM2.	○	○

Answer Area:



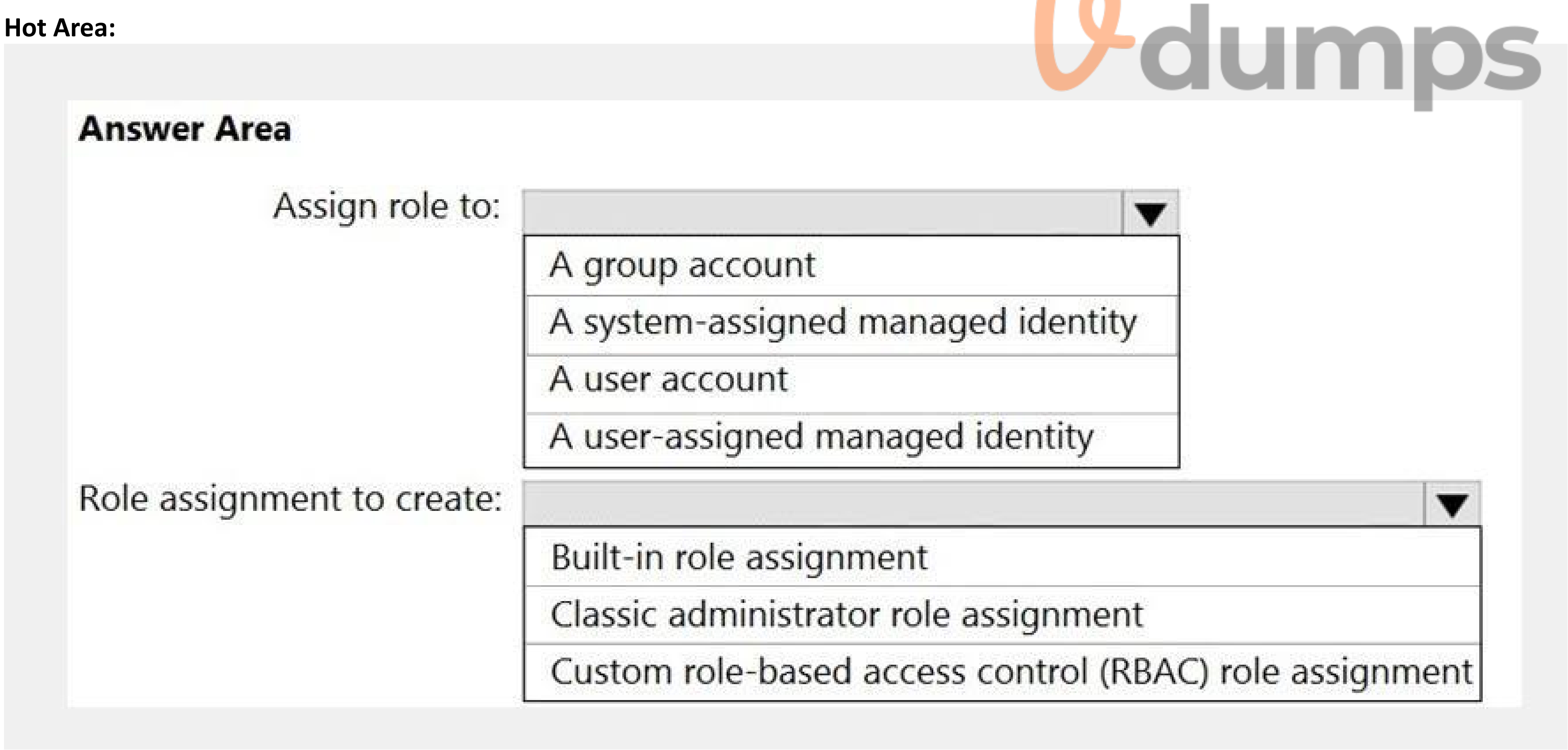
Answer Area

Statements	Yes	No
User1 can deploy virtual machines to RG1.	[✓ ○]	○
User2 can delete VM2.	[✓ ○]	○
User3 can reset the password of the built-in Administrator account of VM2.	○	[✓ ○]

Section:
Explanation:

QUESTION 51
HOTSPOT
You plan to implement an Azure function named Function1 that will create new storage accounts for containerized application instances.
You need to grant Function1 the minimum required privileges to create the storage accounts. The solution must minimize administrative effort.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:

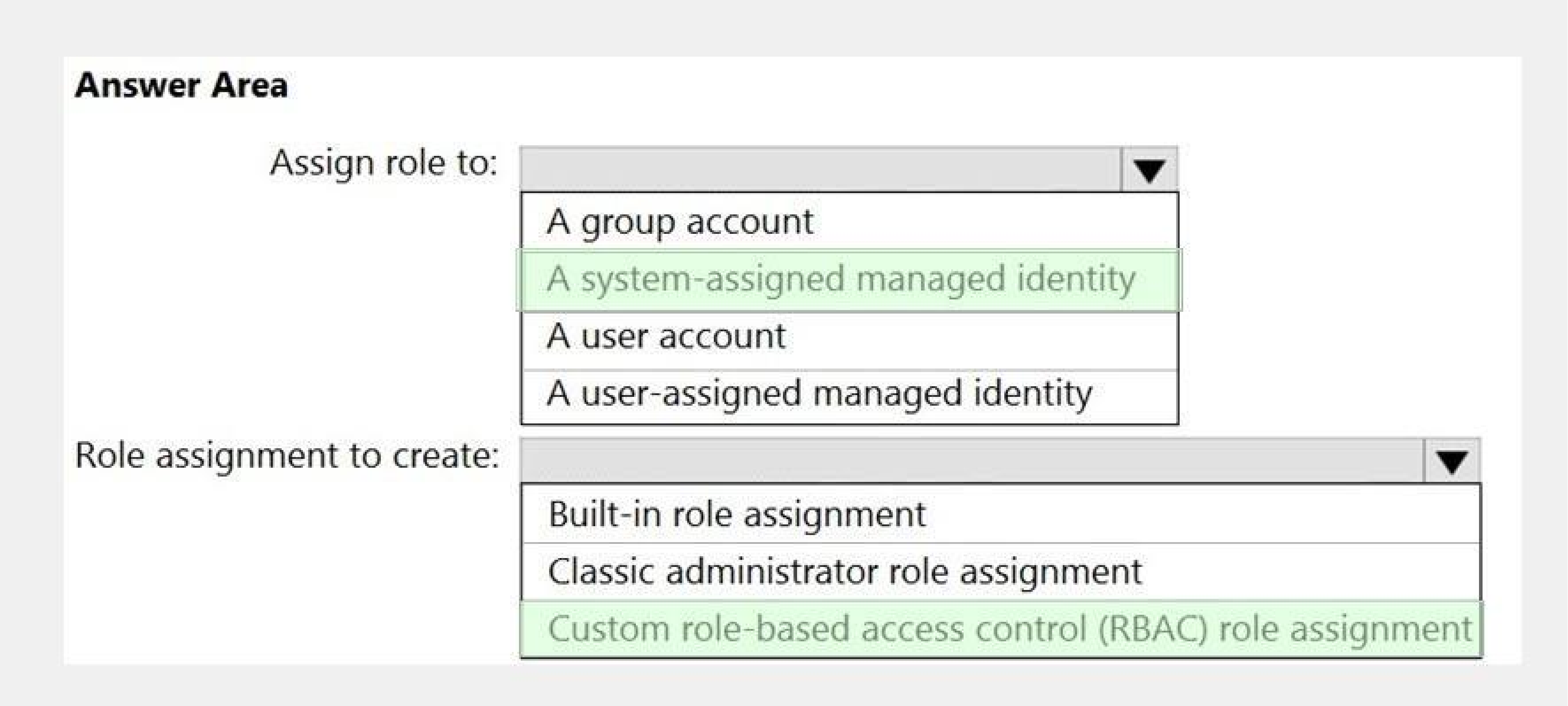


Answer Area

Assign role to: ▼
- A group account
- A system-assigned managed identity
- A user account
- A user-assigned managed identity

Role assignment to create: ▼
- Built-in role assignment
- Classic administrator role assignment
- Custom role-based access control (RBAC) role assignment

Answer Area:



Answer Area

Assign role to:

- A group account
- [✓ A system-assigned managed identity]
- A user account
- A user-assigned managed identity

Role assignment to create:

- Built-in role assignment
- Classic administrator role assignment
- [✓ Custom role-based access control (RBAC) role assignment]

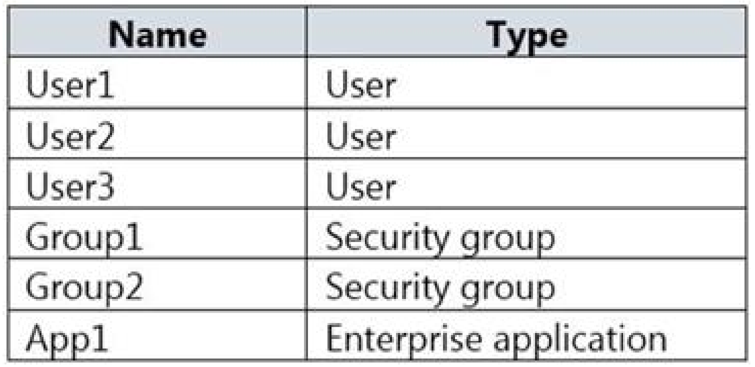
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview
https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/howto-assign-access-portal

QUESTION 52
You have an Azure subscription that is linked to an Azure Active Directory (Azure AD) tenant.
You need to grant Function1 the minimum required privileges.
Which additional resource will be created in Azure AD?

A. a service principal
B. an X.509 certificate
C. a managed identity
D. a user account

Correct Answer: A
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added

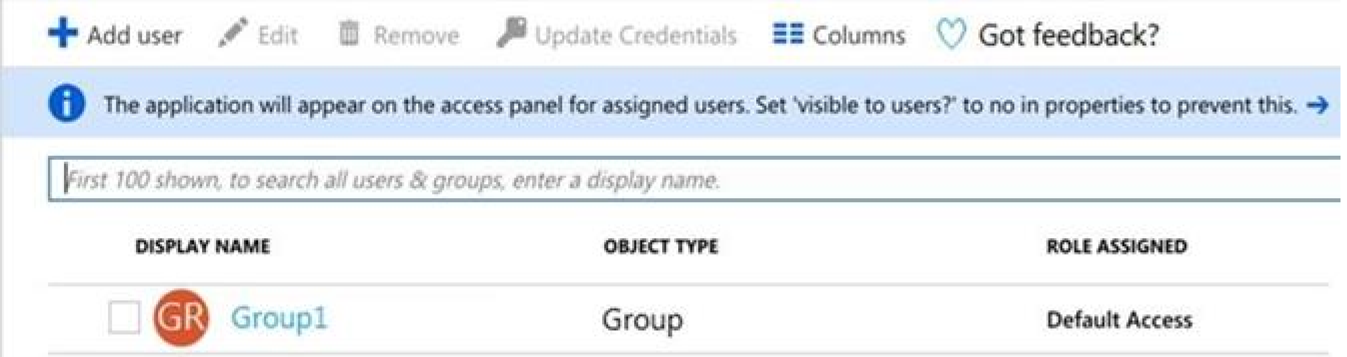
QUESTION 53
HOTSPOT
You have an Azure Active Directory (Azure AD) tenant that contains the resources shown in the following table.



Name	Type
User1	User
User2	User
User3	User
Group1	Security group
Group2	Security group
App1	Enterprise application

User2 is the owner of Group2.

The user and group settings for App1 are configured as shown in the following exhibit.

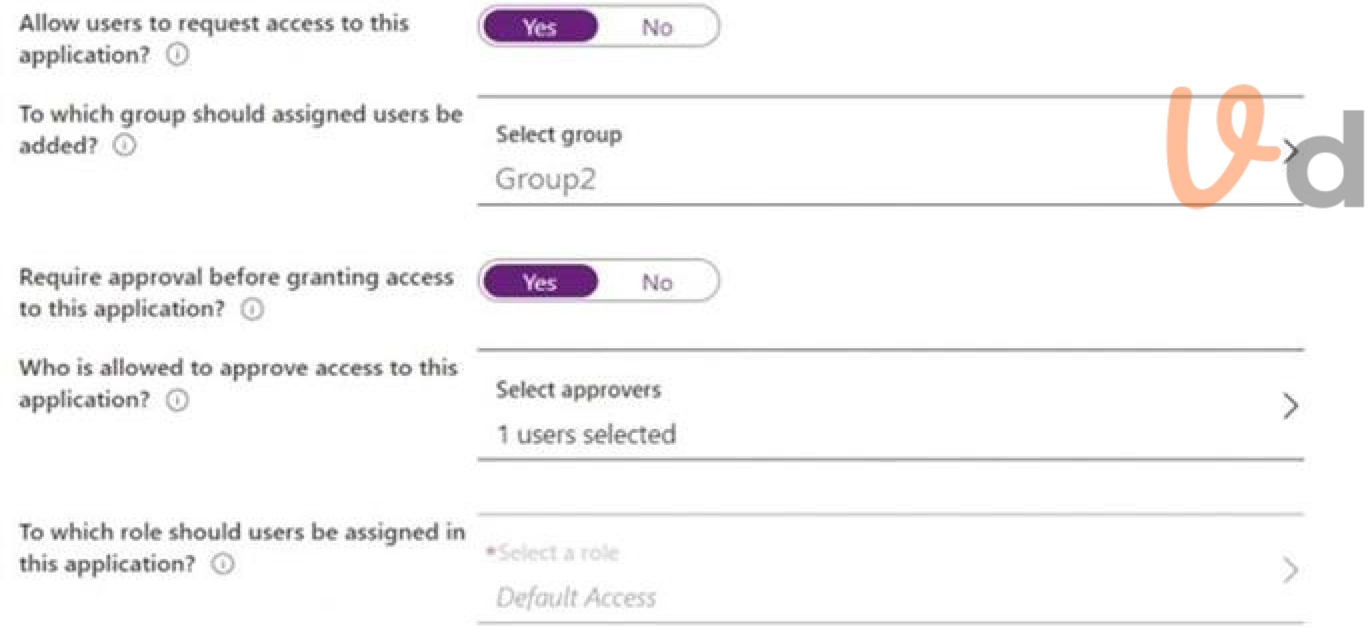


The application will appear on the access panel for assigned users. Set 'visible to users?' to no in properties to prevent this.

First 100 shown, to search all users & groups, enter a display name.

DISPLAY NAME	OBJECT TYPE	ROLE ASSIGNED
□ GR Group1	Group	Default Access

You enable self-service application access for App1 as shown in the following exhibit.



Allow users to request access to this application? ⓘ [✓ Yes] No

To which group should assigned users be added? ⓘ Select group: Group2

Require approval before granting access to this application? ⓘ [✓ Yes] No

Who is allowed to approve access to this application? ⓘ Select approvers: 1 users selected

To which role should users be assigned in this application? ⓘ *Select a role: Default Access

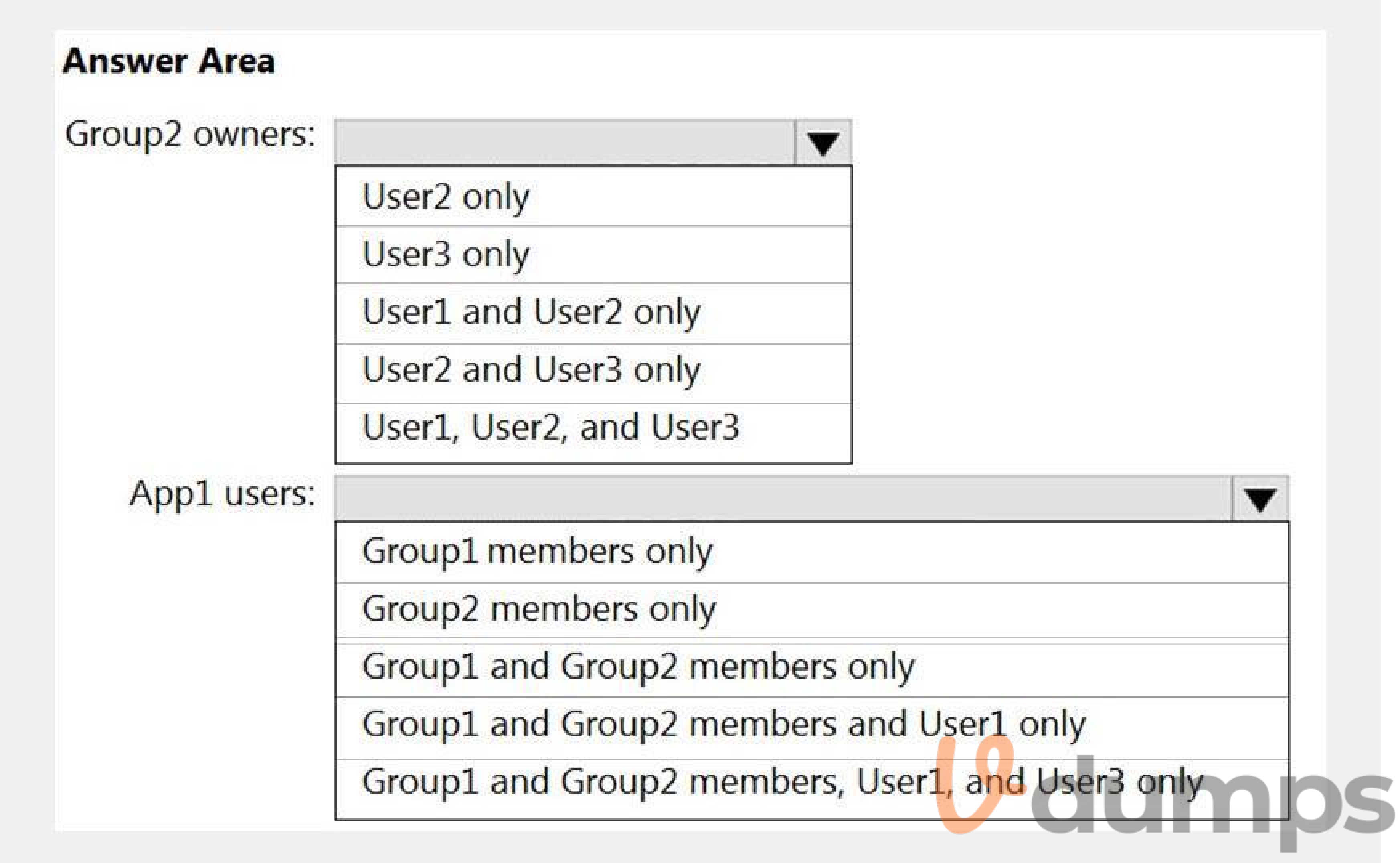
User3 is configured to approve access to Appl.

You need to identify the owners of Group2 and the users of Appl.

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

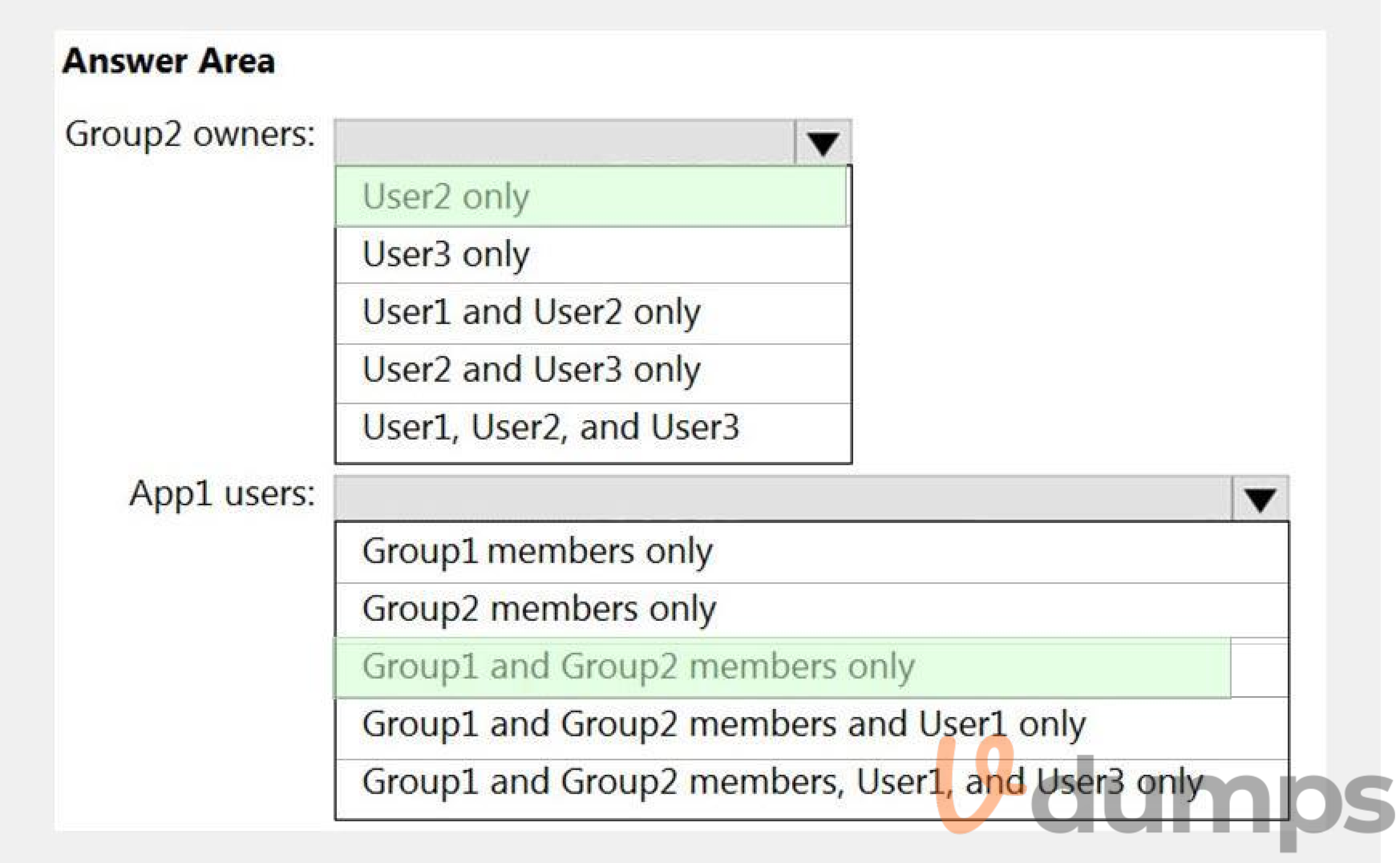
Group2 owners:

- User2 only
- User3 only
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

App1 users:

- Group1 members only
- Group2 members only
- Group1 and Group2 members only
- Group1 and Group2 members and User1 only
- Group1 and Group2 members, User1, and User3 only

Answer Area:



Answer Area

Group2 owners:

- [✓ User2 only]
- User3 only
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

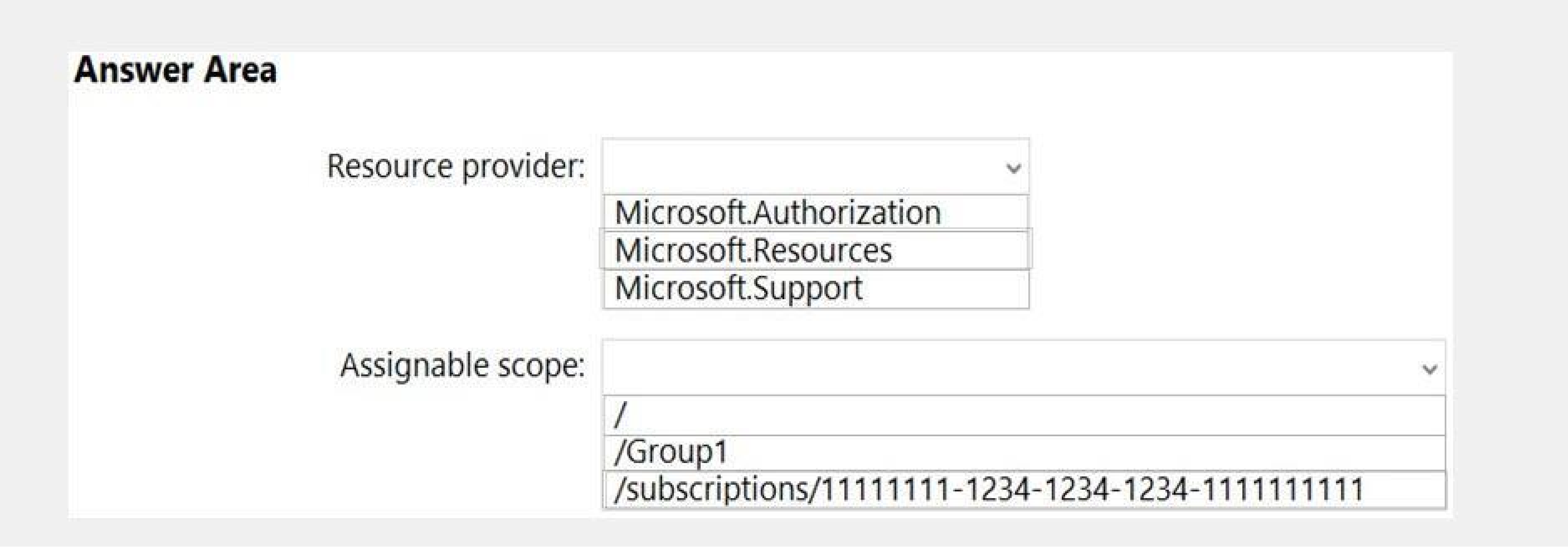
App1 users:

- Group1 members only
- Group2 members only
- [✓ Group1 and Group2 members only]
- Group1 and Group2 members and User1 only
- Group1 and Group2 members, User1, and User3 only

Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/manage-self-service-access

QUESTION 54
HOTSPOT
You have a management group named Group1 that contains an Azure subscription named sub1. Sub1 has a subscription ID of 11111111-1234-1234-1234-1111111111.
You need to create a custom Azure role-based access control (RBAC) role that will delegate permissions to manage the tags on all the objects in Group1.
What should you include in the role definition of Role1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

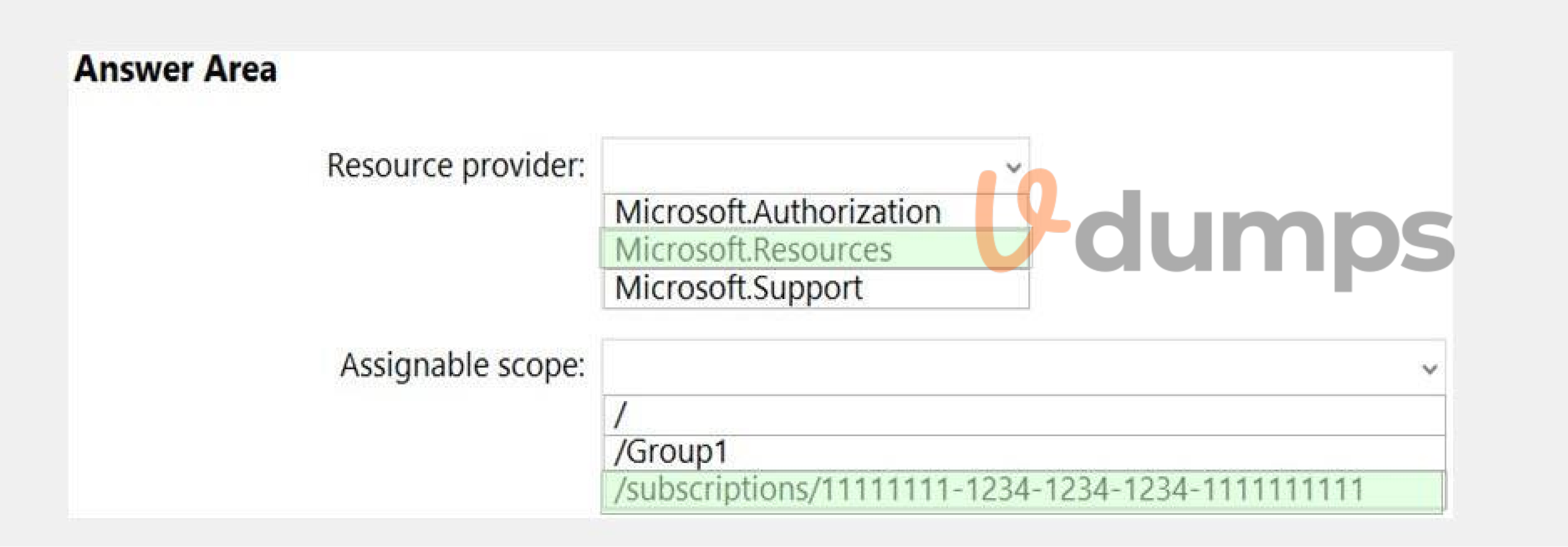
Resource provider:

- Microsoft.Authorization
- Microsoft.Resources
- Microsoft.Support

Assignable scope:

- /
- /Group1
- /subscriptions/11111111-1234-1234-1234-1111111111

Answer Area:



Answer Area

Resource provider:

- Microsoft.Authorization
- [✓ Microsoft.Resources]
- Microsoft.Support

Assignable scope:

- /
- /Group1
- [✓ /subscriptions/11111111-1234-1234-1234-1111111111]

Section:

Explanation:

Note: Assigning a custom RBAC role as the Management Group level is currently in preview only. So, for now the answer to the assignable scope is the subscription level.

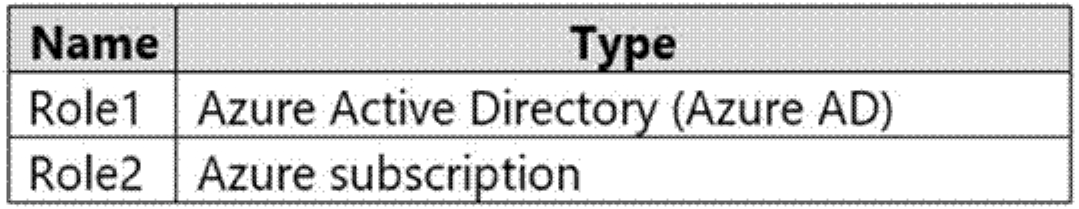
Reference:

https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations
https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles
https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles-portal#step-5-assignable-scopes

QUESTION 55

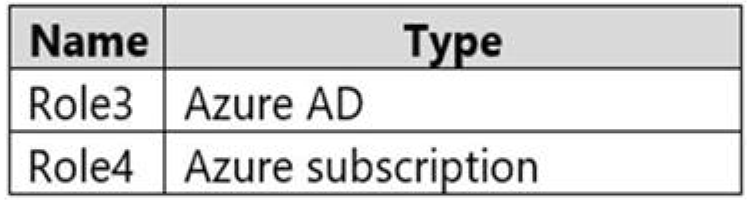
HOTSPOT

You have an Azure subscription that contains the custom roles shown in the following table.



Name	Type
Role1	Azure Active Directory (Azure AD)
Role2	Azure subscription

In the Azure portal, you plan to create new custom roles by cloning existing roles. The new roles will be configured as shown in the following table.

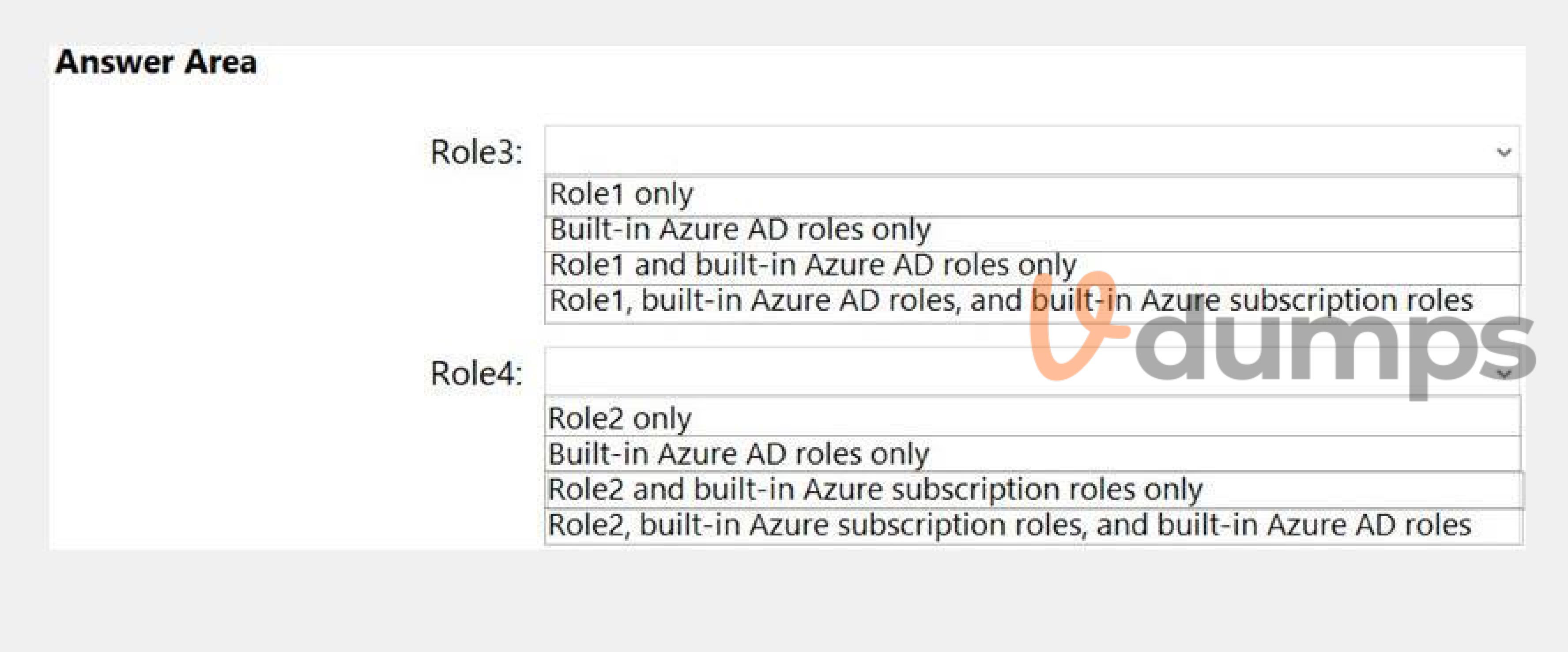


Name	Type
Role3	Azure AD
Role4	Azure subscription

Which roles can you clone to create each new role? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

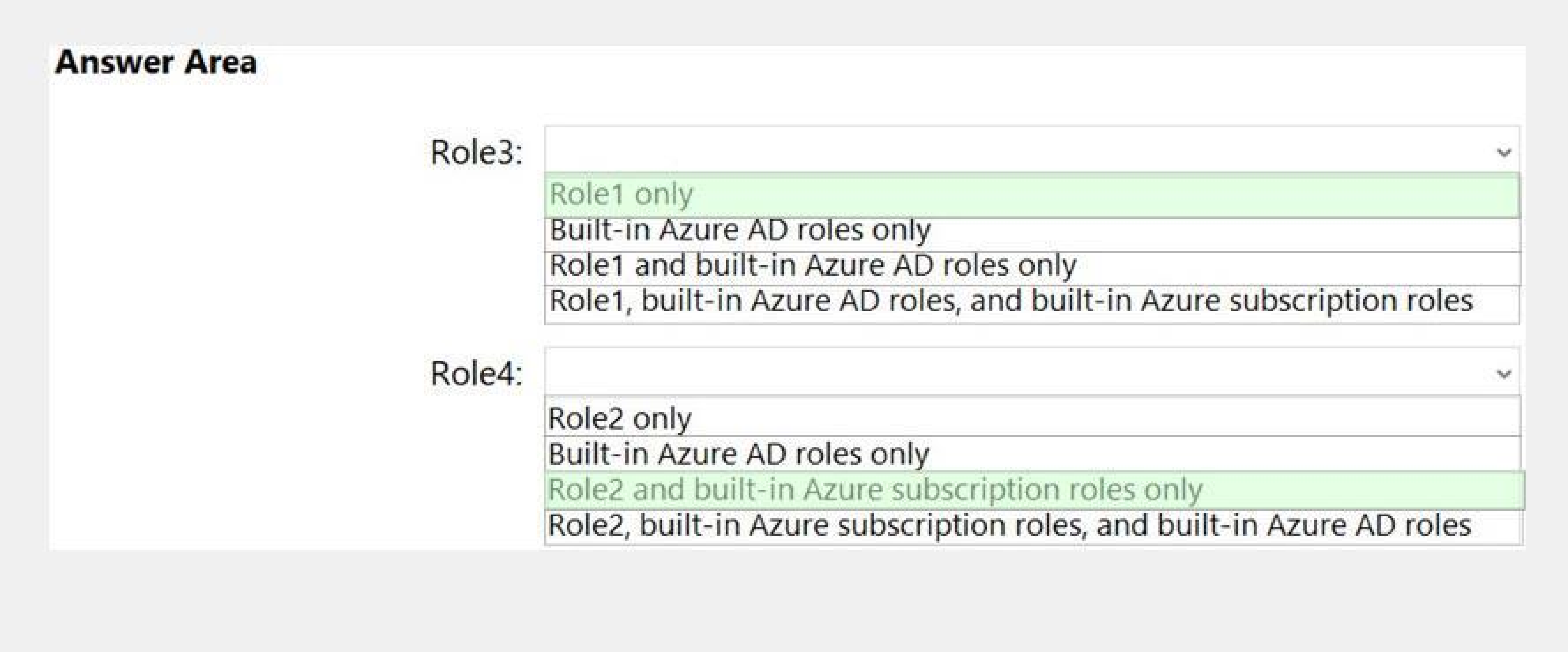


Answer Area

Role3:
- Role1 only
- Built-in Azure AD roles only
- Role1 and built-in Azure AD roles only
- Role1, built-in Azure AD roles, and built-in Azure subscription roles

Role4:
- Role2 only
- Built-in Azure AD roles only
- Role2 and built-in Azure subscription roles only
- Role2, built-in Azure subscription roles, and built-in Azure AD roles

Answer Area:



Answer Area

Role3:

[✓ Role1 only]
Built-in Azure AD roles only
Role1 and built-in Azure AD roles only
Role1, built-in Azure AD roles, and built-in Azure subscription roles

Role4:

Role2 only
Built-in Azure AD roles only
[✓ Role2 and built-in Azure subscription roles only]
Role2, built-in Azure subscription roles, and built-in Azure AD roles

Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/roles/custom-create
https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles-portal

QUESTION 56
HOTSPOT
You have an Azure subscription that contains the Azure Active Directory (Azure AD) resources shown in the following table.

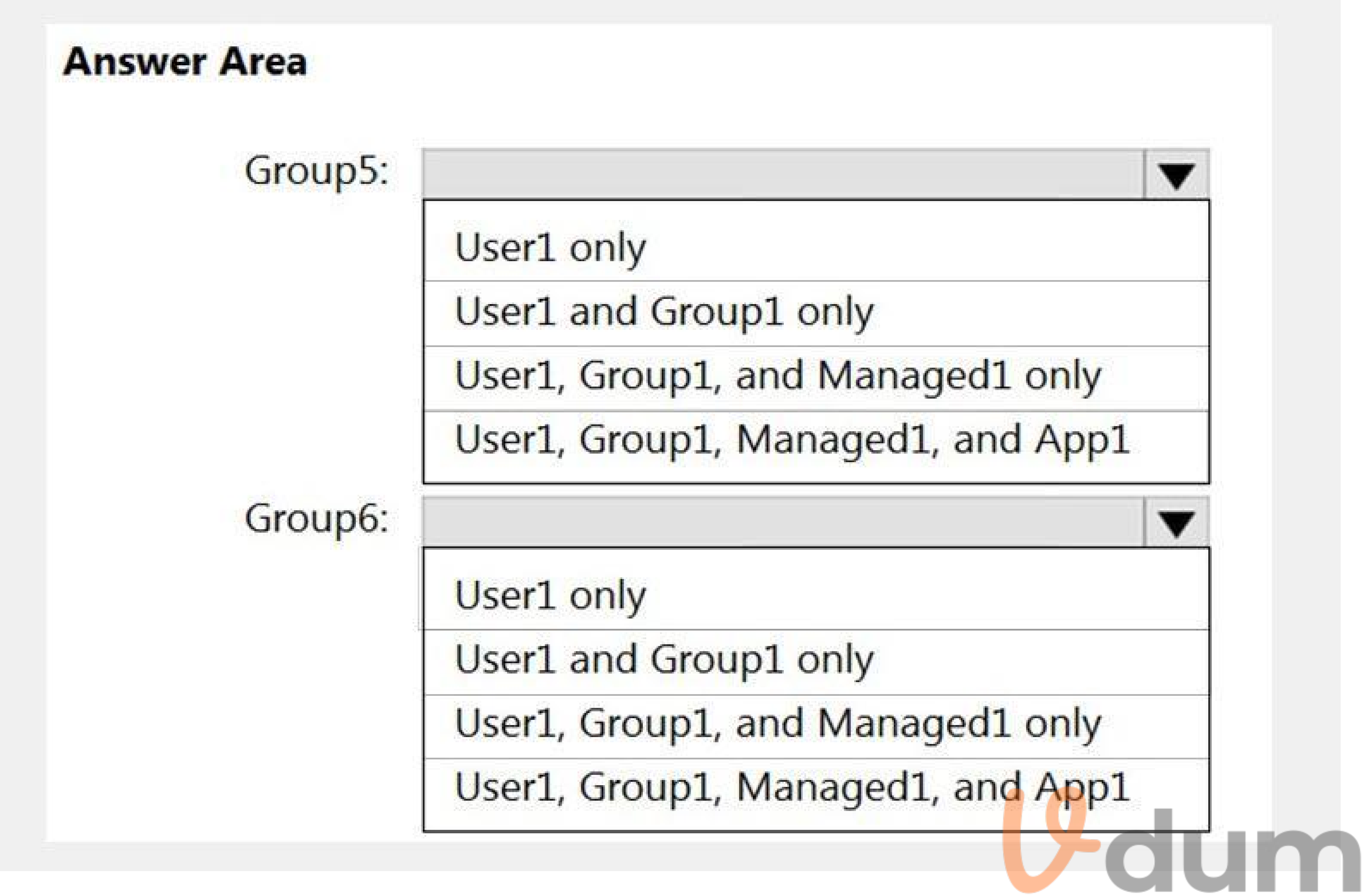
Name	Description
User1	User
Group1	Security group that has a Membership type of Dynamic Device
Managed1	Managed identity
App1	Enterprise application

You create the groups shown in the following table.

Name	Description
Group5	Security group that has a Membership type of Assigned
Group6	Microsoft 365 group that has a Membership type of Assigned

Which resources can you add to Group5 and Group6? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

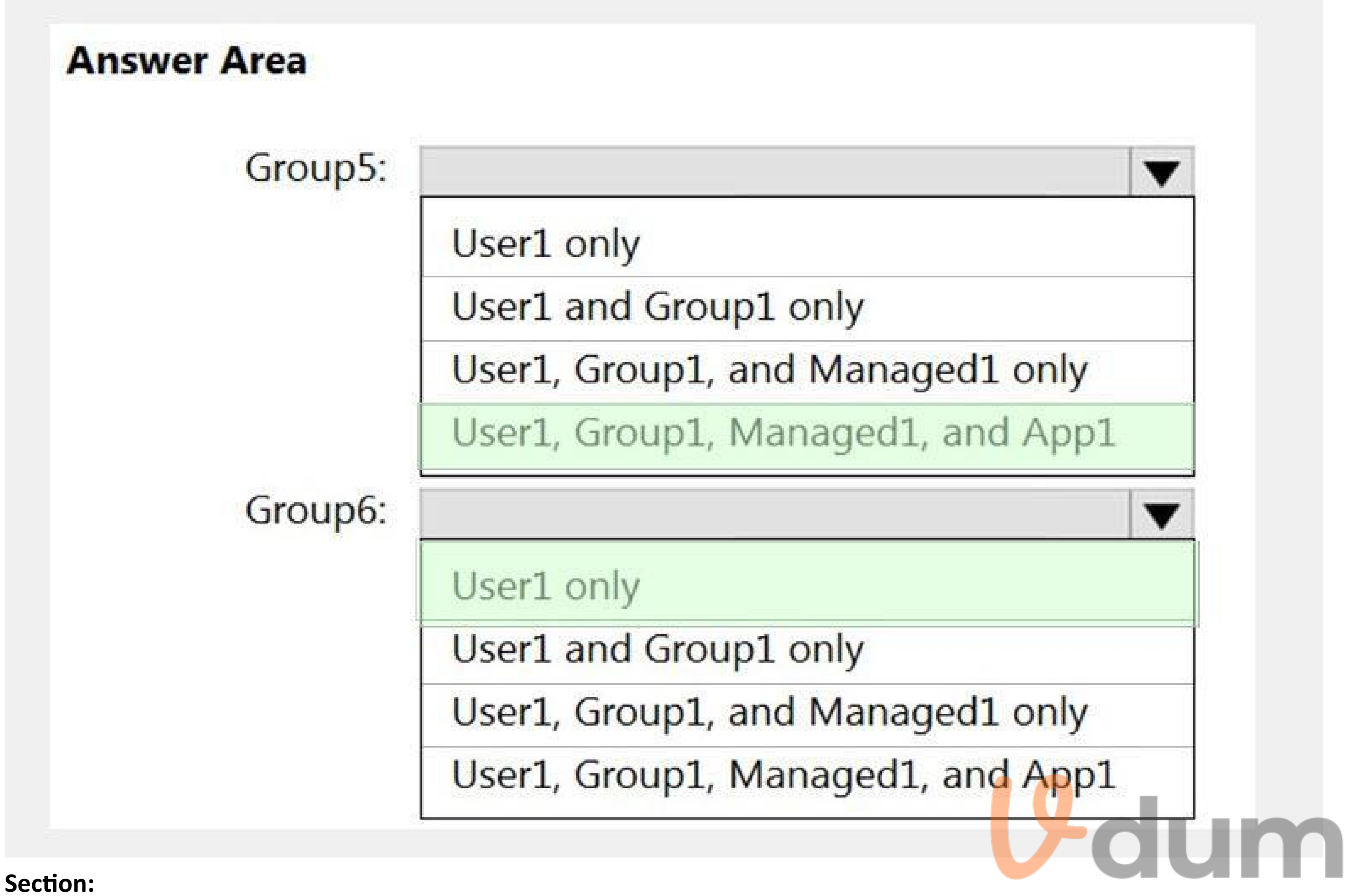
Group5:

- User1 only
- User1 and Group1 only
- User1, Group1, and Managed1 only
- User1, Group1, Managed1, and App1

Group6:

- User1 only
- User1 and Group1 only
- User1, Group1, and Managed1 only
- User1, Group1, Managed1, and App1

Answer Area:



Answer Area

Group5:

- User1 only
- User1 and Group1 only
- User1, Group1, and Managed1 only
- [✓ User1, Group1, Managed1, and App1]

Group6:

- [✓ User1 only]
- User1 and Group1 only
- User1, Group1, and Managed1 only
- User1, Group1, Managed1, and App1

Section:
Explanation:

QUESTION 57

HOTSPOT

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains three security groups named Group1, Group2, and Group3 and the users shown in the following table.

Name	Role	Member of
User1	Application administrator	Group1
User2	Application developer	Group2
User3	Cloud application administrator	Group3

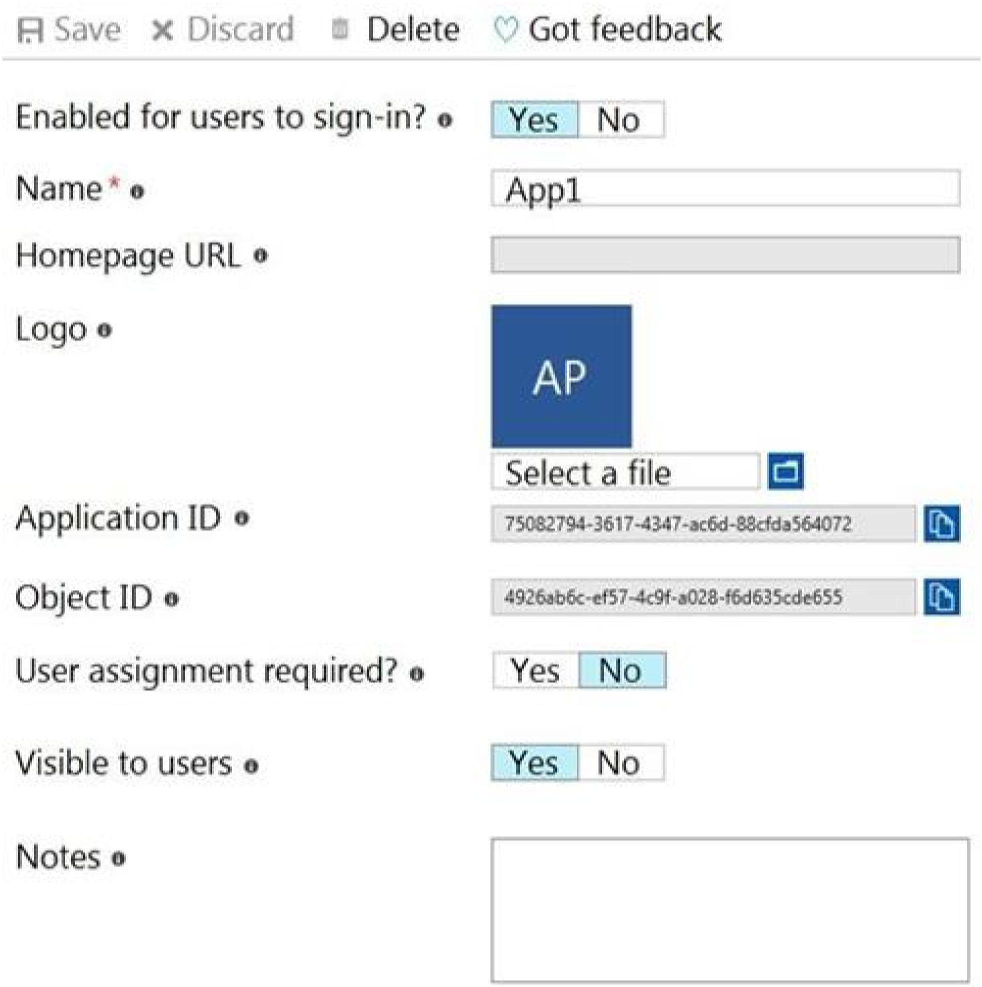
Group3 is a member of Group2.

In contoso.com, you register an enterprise application named App1 that has the following settings:

Owners: User1

Users and groups: Group2

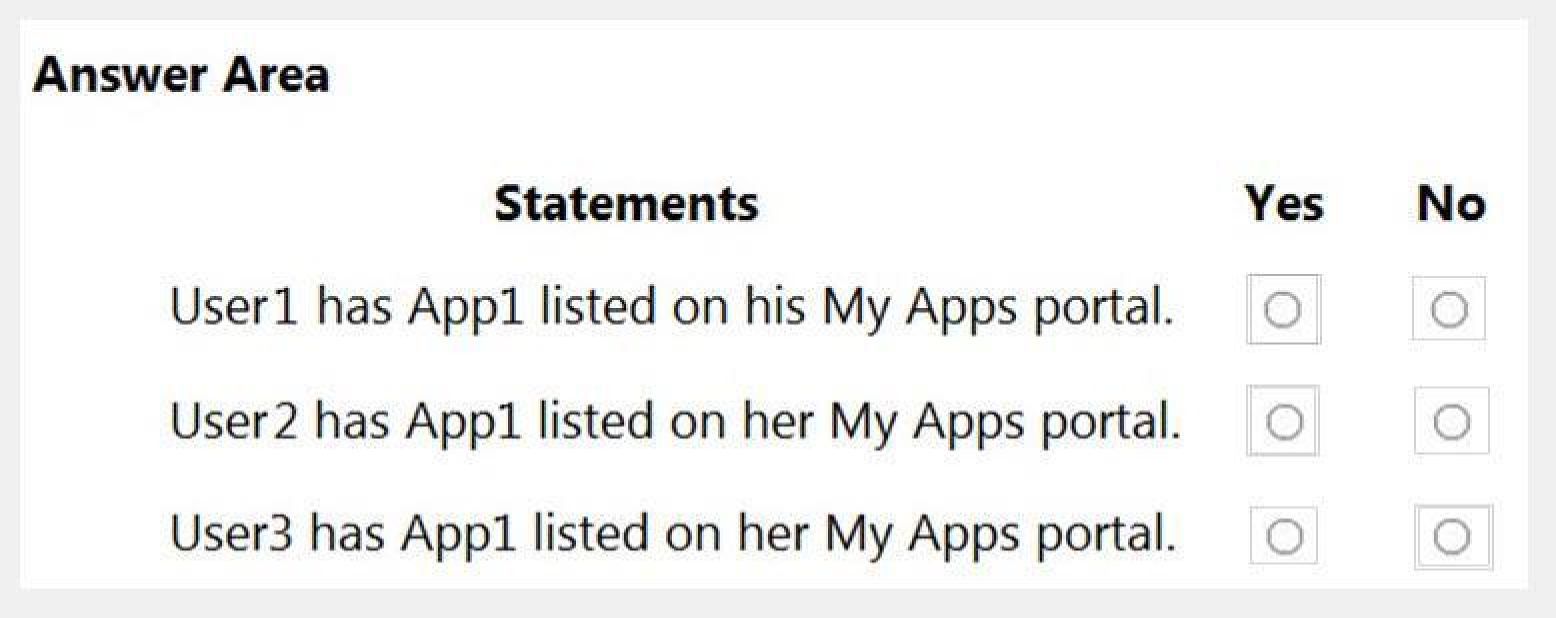
You configure the properties of App1 as shown in the following exhibit.



Enabled for users to sign-in?	[✓ Yes] No
Name*	App1
Homepage URL	
Logo	AP Select a file
Application ID	75082794-3617-4347-ac6d-88cfda564072
Object ID	4926ab6c-ef57-4c9f-a028-f6d635cde655
User assignment required?	Yes [✓ No]
Visible to users	[✓ Yes] No
Notes	

For each of the following statements, select Yes if the statement is true. Otherwise, select no.
NOTE: Each correct selection is worth one point.

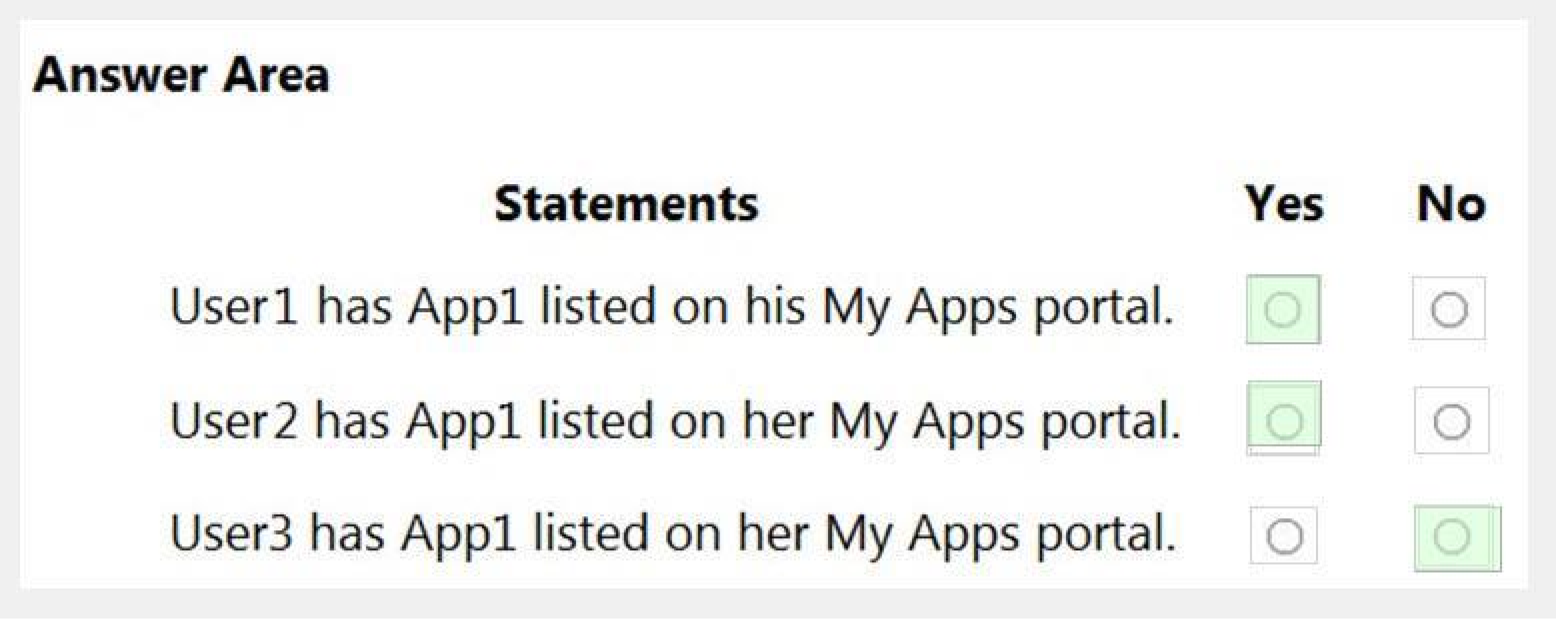
Hot Area:



Answer Area

Statements	Yes	No
User1 has App1 listed on his My Apps portal.	○	○
User2 has App1 listed on her My Apps portal.	○	○
User3 has App1 listed on her My Apps portal.	○	○

Answer Area:



Answer Area

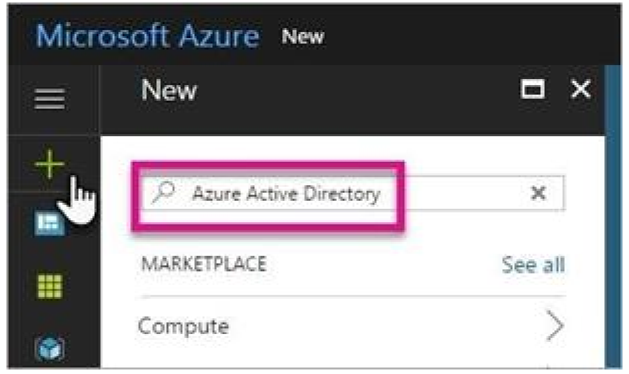
Statements	Yes	No
User1 has App1 listed on his My Apps portal.	[✓ ○]	○
User2 has App1 listed on her My Apps portal.	[✓ ○]	○
User3 has App1 listed on her My Apps portal.	○	[✓ ○]

Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal

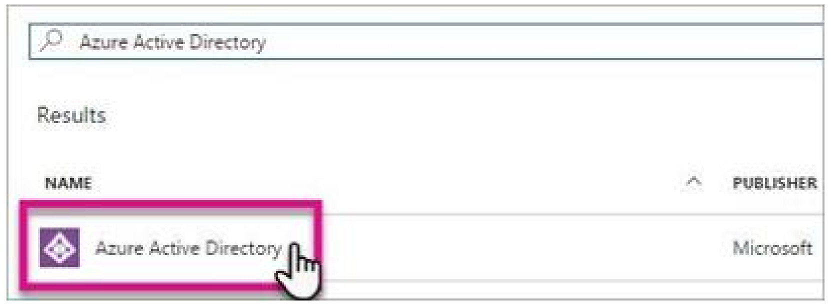
QUESTION 58
SIMULATION
You need to create a new Azure Active Directory (Azure AD) directory named 10317806.onmicrosoft.com. The new directory must contain a user named user10317806 who is configured to sign in by using Azure Multi-Factor Authentication (MFA).

A.

Correct Answer: A
Section:
Explanation:
Answer: A
Explanation:
To create a new Azure AD tenant:
1. Browse to the Azure portal and sign in with an account that has an Azure subscription.
2. Select the plus icon (+) and search for Azure Active Directory.

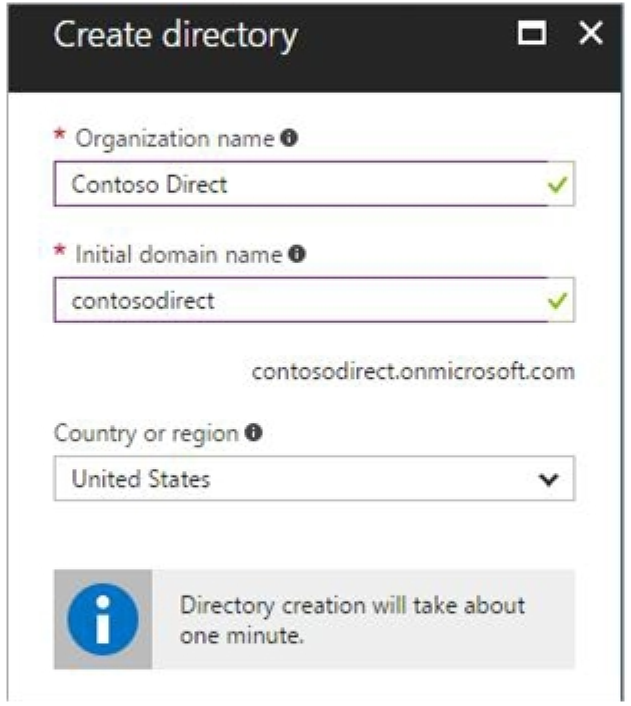


3. Select Azure Active Directory in the search results.



4. Select Create.

5. Provide an Organization name (10317806) and an Initial domain name (10317806). Then select Create. This will create the directory named 10317806.onmicrosoft.com.



Create directory

* Organization name: Contoso Direct

* Initial domain name: contosodirect

contosodirect.onmicrosoft.com

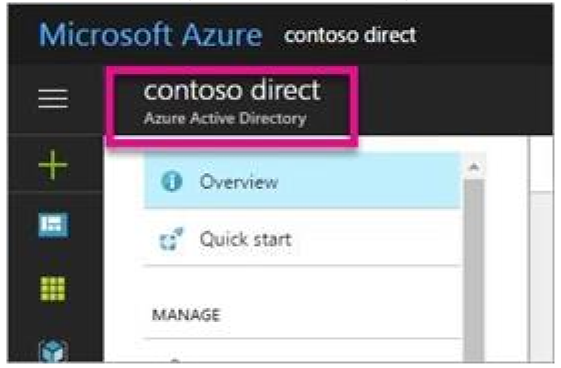
Country or region: United States

Directory creation will take about one minute.

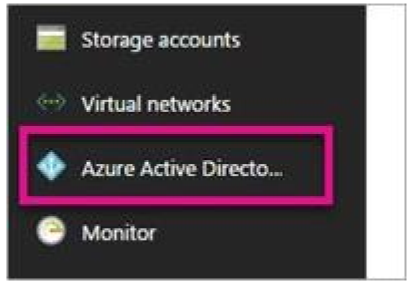
6. After directory creation is complete, select the information box to manage your new directory.

To create the user:

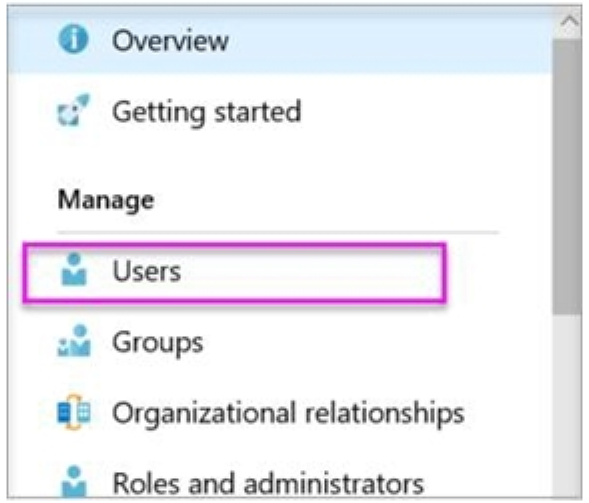
1. In the Azure portal, make sure you are on the Azure Active Directory fly out.



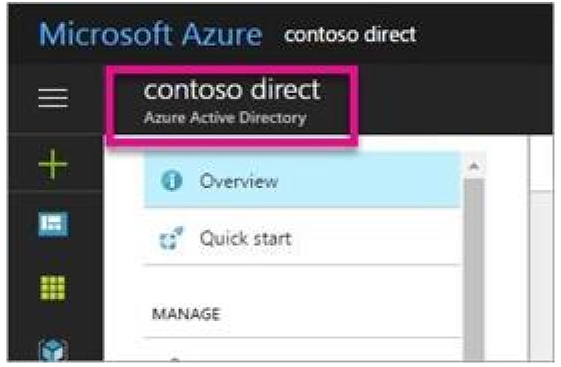
If not, select the Azure Active Directory icon from the left services navigation.



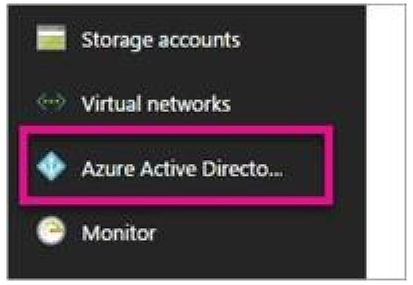
2. Under Manage, select Users.



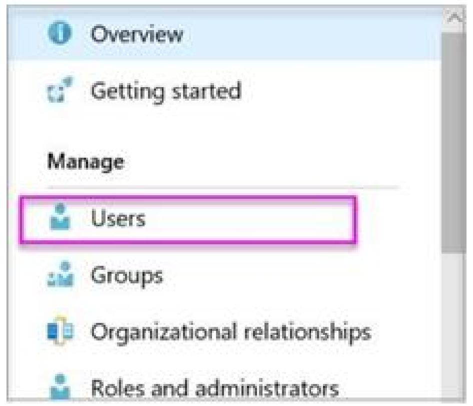
3. Select All users and then select + New user.
4. Provide a Name and User name (user10317806) for the user. When you're done, select Create.
To enable MFA:
1. In the Azure portal, make sure you are on the Azure Active Directory fly out.



If not, select the Azure Active Directory icon from the left services navigation.



2. Under Manage, select Users.



3. Click on the Multi-Factor Authentication link.
4. Tick the checkbox next to the user's name and click the Enable link.
Reference:
https://docs.microsoft.com/en-us/power-bi/developer/create-an-azure-active-directory-tenant

QUESTION 59
You have an Azure subscription named Subcription1 that contains an Azure Active Directory (Azure AD) tenant named contoso.com and a resource group named RG1.
You create a custom role named Role1 for contoso.com.
Where you can use Role1 for permission delegation?

A. contoso.com only
B. contoso.com and RG1 only
C. contoso.com and Subscription1 only
D. contoso.com, RG1, and Subscription1

Correct Answer: D
Section:

QUESTION 60
You have an Azure subscription.
You enable Azure Active Directory (Azure AD) Privileged Identity Management (PIM).
Your company's security policy for administrator accounts has the following conditions:
The accounts must use multi-factor authentication (MFA).
The accounts must use 20-character complex passwords.
The passwords must be changed every 180 days.
The accounts must be managed by using PIM.
You receive multiple alerts about administrators who have not changed their password during the last 90 days.
You need to minimize the number of generated alerts.
Which PIM alert should you modify?

A. Roles are being assigned outside of Privileged Identity Management
B. Roles don't require multi-factor authentication for activation
C. Administrators aren't using their privileged roles
D. Potential stale accounts in a privileged role

Correct Answer: D
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-configure-security-alerts?tabs=new

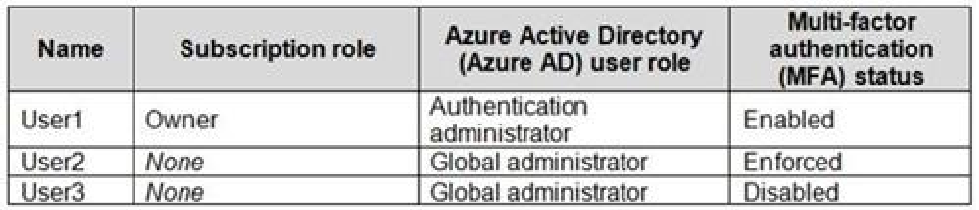
QUESTION 61
Your network contains an on-premises Active Directory domain named adatum.com that syncs to Azure Active Directory (Azure AD). Azure AD Connect is installed on a domain member server named Server1.
You need to ensure that a domain administrator for the adatum.com domain can modify the synchronization options. The solution must use the principle of least privilege. Which Azure AD role should you assign to the domain administrator?

A. Security administrator
B. Global administrator
C. User administrator

Correct Answer: B
Section:
Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-accounts-permissions

QUESTION 62
You have an Azure subscription that contains the users shown in the following table.



Name	Subscription role	Azure Active Directory (Azure AD) user role	Multi-factor authentication (MFA) status
User1	Owner	Authentication administrator	Enabled
User2	*None*	Global administrator	Enforced
User3	*None*	Global administrator	Disabled

Which users can enable Azure AD Privileged Identity Management (PIM)?

A. User2 and User3 only
B. User1 and User2 only
C. User2 only
D. User1 only

Correct Answer: D
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-deployment-plan

QUESTION 63
You have an Azure subscription.
You plan to create a custom role-based access control (RBAC) role that will provide permission to read the Azure Storage account.
Which property of the RBAC role definition should you configure?

A. NotActions []
B. DataActions []
C. AssignableScopes []
D. Actions []

Correct Answer: D
Section:
Explanation:
To ‘Read a storage account’, ie. list the blobs in the storage account, you need an ‘Action’ permission. To read the data in a storage account, ie. open a blob, you need a ‘DataAction’ permission.
Reference:
https://docs.microsoft.com/en-us/azure/role-based-access-control/role-definitions

01 - Implement platform protection
This is a case study.
Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.
To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.
At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

General Overview

Fabrikam, Inc. is a consulting company that has a main office in Montreal and branch offices in Seattle and New York. Fabrikam has IT, human resources (HR), and finance departments.

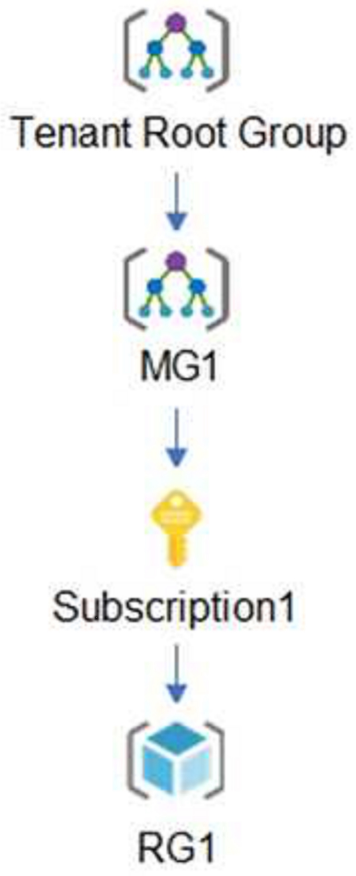
Existing Environment

Network Environment

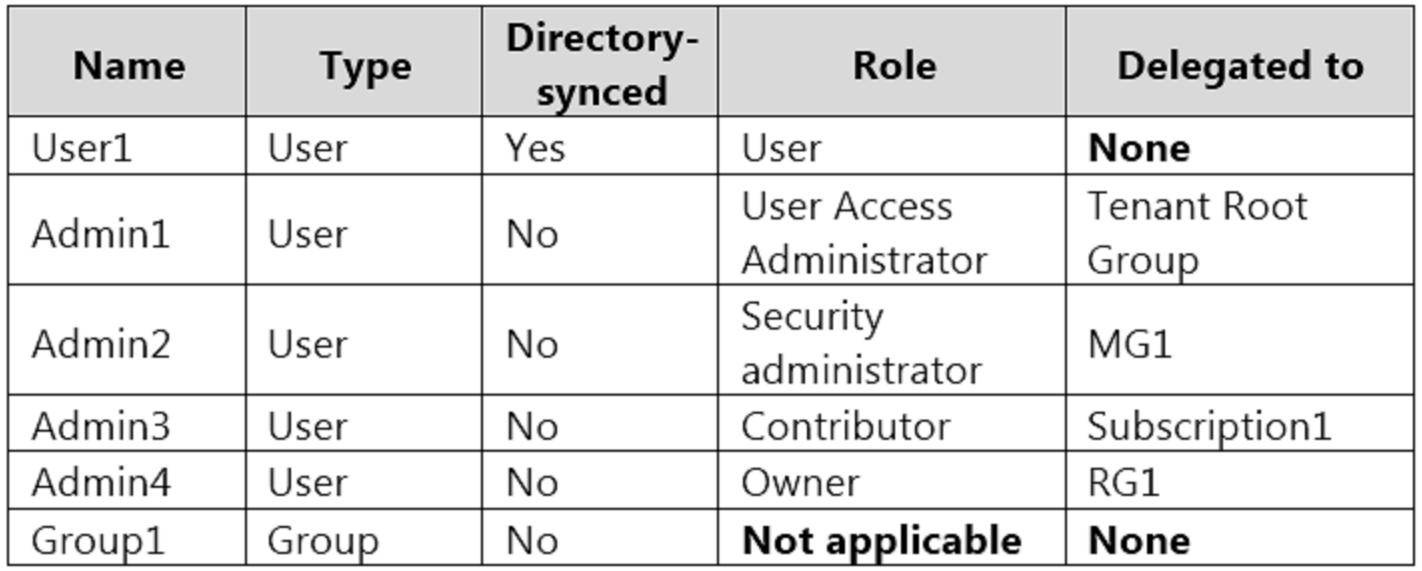
Fabrikam has a Microsoft 365 subscription and an Azure subscription named subscription1.

The network contains an on-premises Active Directory domain named Fabrikam.com. The domain contains two organizational units (OUs) named OU1 and OU2. Azure AD Connect cloud sync syncs only OU1.

The Azure resources hierarchy is shown in the following exhibit.

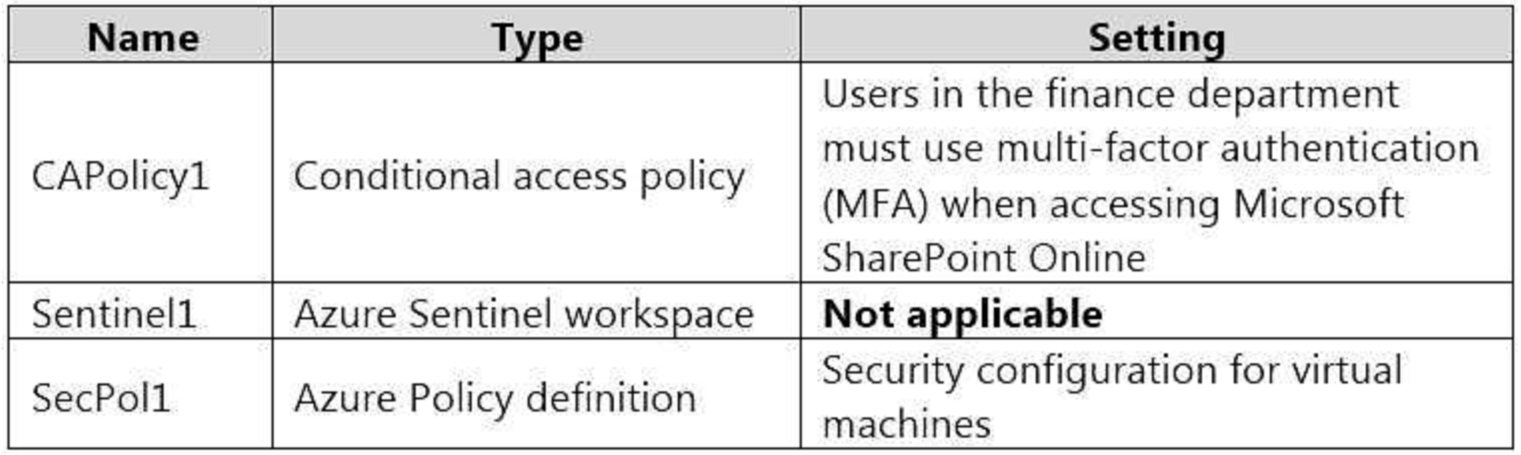


The Azure Active Directory (Azure AD) tenant contains the users shown in the following table.



Name	Type	Directory-synced	Role	Delegated to
User1	User	Yes	User	**None**
Admin1	User	No	User Access Administrator	Tenant Root Group
Admin2	User	No	Security administrator	MG1
Admin3	User	No	Contributor	Subscription1
Admin4	User	No	Owner	RG1
Group1	Group	No	**Not applicable**	**None**

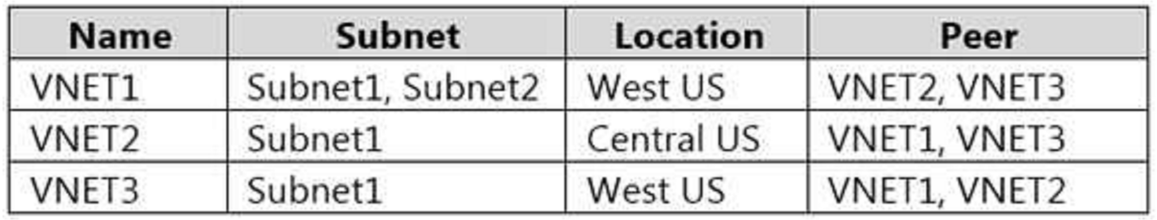
Azure AD contains the resources shown in the following table.



Name	Type	Setting
CAPolicy1	Conditional access policy	Users in the finance department must use multi-factor authentication (MFA) when accessing Microsoft SharePoint Online
Sentinel1	Azure Sentinel workspace	**Not applicable**
SecPol1	Azure Policy definition	Security configuration for virtual machines

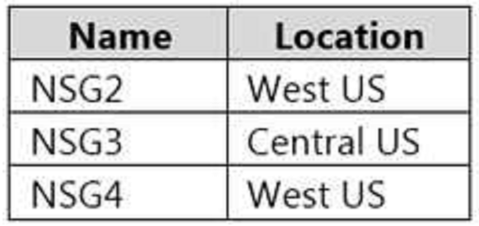
Subscription1 Resources

Subscription1 contains the virtual networks shown in the following table.



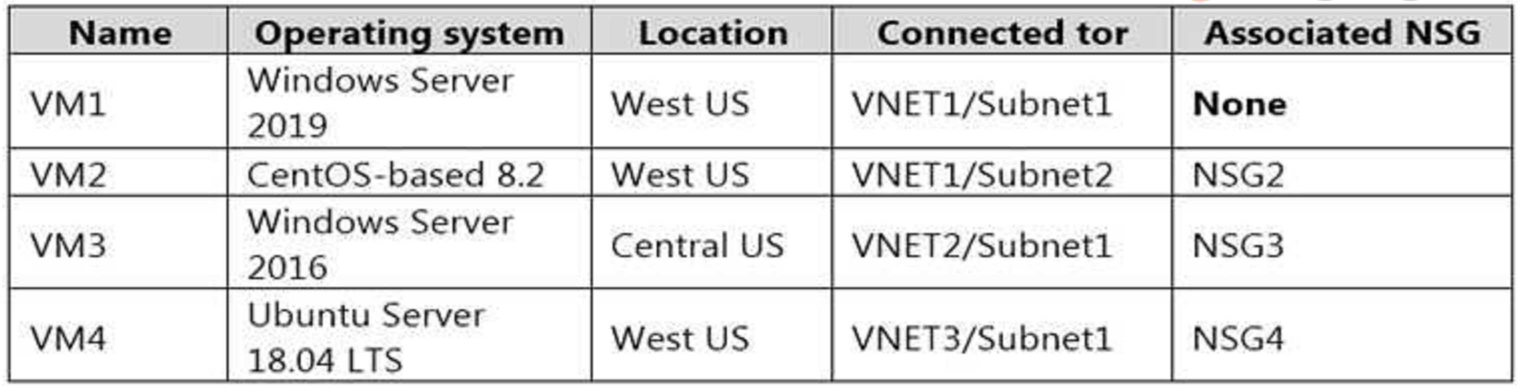
Name	Subnet	Location	Peer
VNET1	Subnet1, Subnet2	West US	VNET2, VNET3
VNET2	Subnet1	Central US	VNET1, VNET3
VNET3	Subnet1	West US	VNET1, VNET2

Subscription1 contains the network security groups (NSGs) shown in the following table.



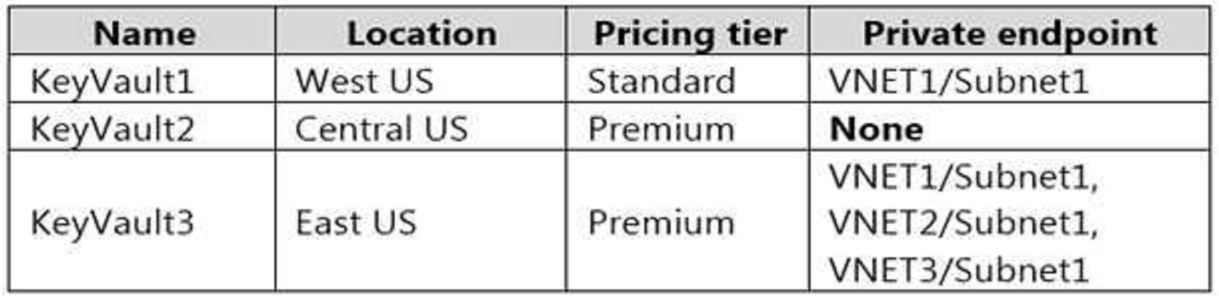
Name	Location
NSG2	West US
NSG3	Central US
NSG4	West US

Subscription1 contains the virtual machines shown in the following table.



Name	Operating system	Location	Connected tor	Associated NSG
VM1	Windows Server 2019	West US	VNET1/Subnet1	**None**
VM2	CentOS-based 8.2	West US	VNET1/Subnet2	NSG2
VM3	Windows Server 2016	Central US	VNET2/Subnet1	NSG3
VM4	Ubuntu Server 18.04 LTS	West US	VNET3/Subnet1	NSG4

Subscription1 contains the Azure key vaults shown in the following table.



Name	Location	Pricing tier	Private endpoint
KeyVault1	West US	Standard	VNET1/Subnet1
KeyVault2	Central US	Premium	**None**
KeyVault3	East US	Premium	VNET1/Subnet1, VNET2/Subnet1, VNET3/Subnet1

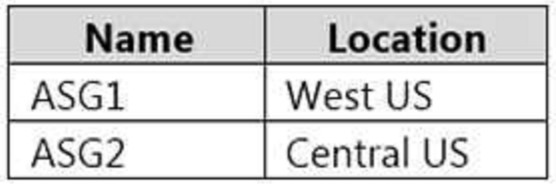
Subscription1 contains a storage account named storage1 in the West US Azure region.

Planned Changes and Requirements

Planned Changes

Fabrikam plans to implement the following changes:

Create two application security groups as shown in the following table.



Name	Location
ASG1	West US
ASG2	Central US

Associate the network interface of VM1 to ASG1.
Deploy SecPol1 by using Azure Security Center.
Deploy a third-party app named App1. A version of App1 exists for all available operating systems.
Create a resource group named RG2.
Sync OU2 to Azure AD.
Add User1 to Group1.
Technical Requirements
Fabrikam identifies the following technical requirements:
The finance department users must reauthenticate after three hours when they access SharePoint Online. Storage1 must be encrypted by using customer-managed keys and automatic key rotation.
From Sentinel1, you must ensure that the following notebooks can be launched:

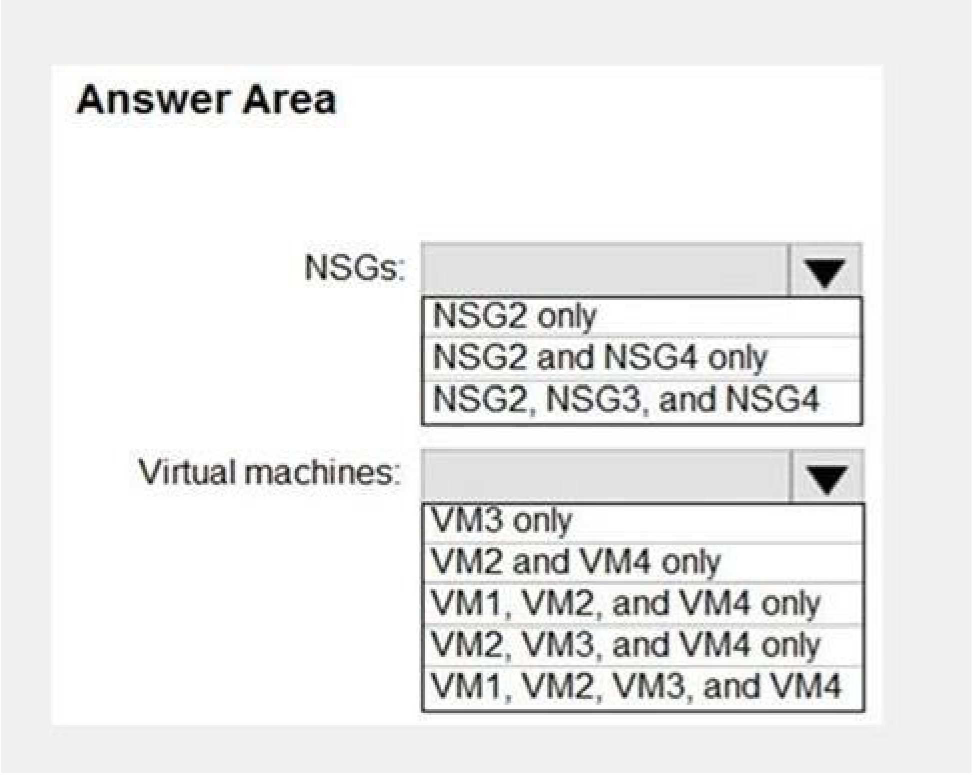
- Entity Explorer – Account
- Entity Explorer – Windows Host
- Guided Investigation Process Alerts

VM1, VM2, and VM3 must be encrypted by using Azure Disk Encryption.
Just in time (JIT) VM access for VM1, VM2, and VM3 must be enabled.
App1 must use a secure connection string stored in KeyVault1.
KeyVault1 traffic must NOT travel over the internet.

QUESTION 1

HOTSPOT
You implement the planned changes for ASG1 and ASG2.
In which NSGs can you use ASG1, and the network interfaces of which virtual machines can you assign to ASG2?

Hot Area:

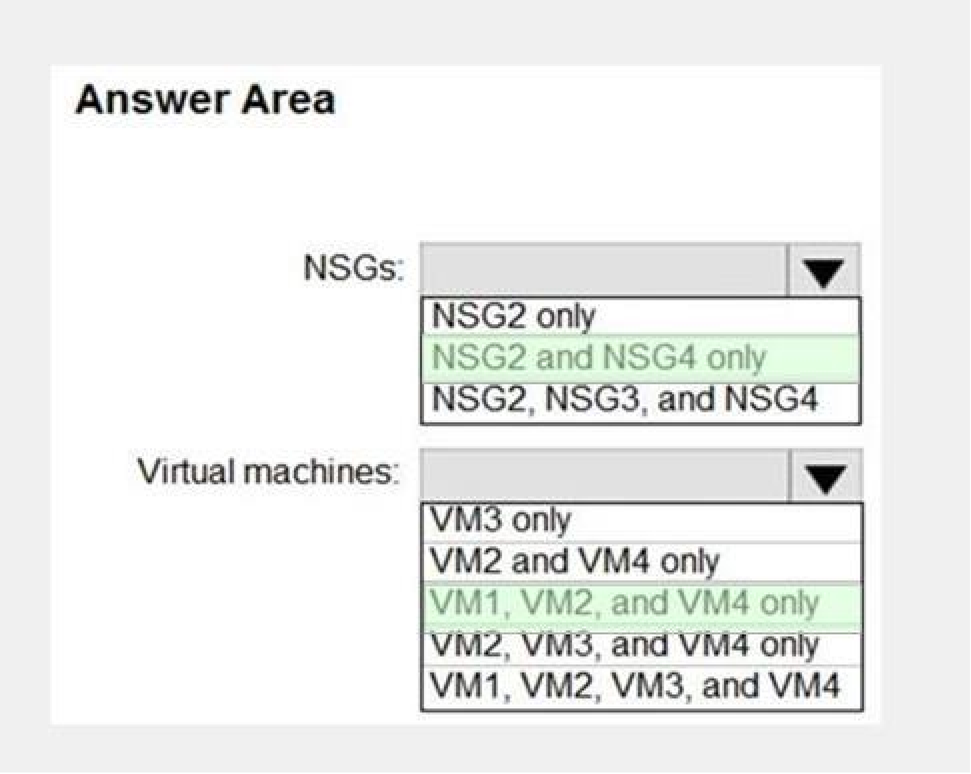


Answer Area

NSGs:
- NSG2 only
- NSG2 and NSG4 only
- NSG2, NSG3, and NSG4

Virtual machines:
- VM3 only
- VM2 and VM4 only
- VM1, VM2, and VM4 only
- VM2, VM3, and VM4 only
- VM1, VM2, VM3, and VM4

Answer Area:



Answer Area

NSGs:
- NSG2 only
- [✓ NSG2 and NSG4 only]
- NSG2, NSG3, and NSG4

Virtual machines:
- VM3 only
- VM2 and VM4 only
- [✓ VM1, VM2, and VM4 only]
- VM2, VM3, and VM4 only
- VM1, VM2, VM3, and VM4

Section:
Explanation:

QUESTION 2
You plan to implement JIT VM access.
Which virtual machines will be supported?

A. VM2, VM3, and VM4 only
B. VM1, VM2, VM3, and VM4
C. VM1 and VM3 only
D. VM1 only

Correct Answer: C
Section:

QUESTION 3
You plan to configure Azure Disk Encryption for VM4.
Which key vault can you use to store the encryption key?

A. KeyVault1
B. KeyVault2
C. KeyVault3

Correct Answer: A
Section:
Explanation:
The key vault needs to be in the same subscription and same region as the VM.
VM4 is in West US. KeyVault1 is the only key vault in the same region as the VM.
Reference: https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-key-vault

QUESTION 4

You need to encrypt storage1 to meet the technical requirements.
Which key vaults can you use?

A. KeyVault2 and KeyVault3 only
B. KeyVault1 only
C. KeyVault1 and KeyVault3 only
D. KeyVault1, KeyVault2, and KeyVault3

Correct Answer: A
Section:
Explanation:

02 - Implement platform protection

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

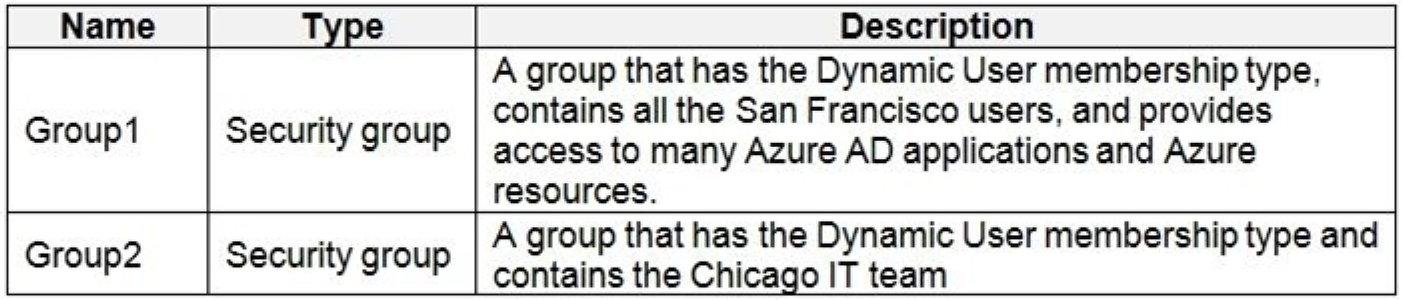
Litware, Inc. is a digital media company that has 500 employees in the Chicago area and 20 employees in the San Francisco area.

Existing Environment

Litware has an Azure subscription named Sub1 that has a subscription ID of 43894a43-17c2-4a39-8cfc-3540c2653ef4.

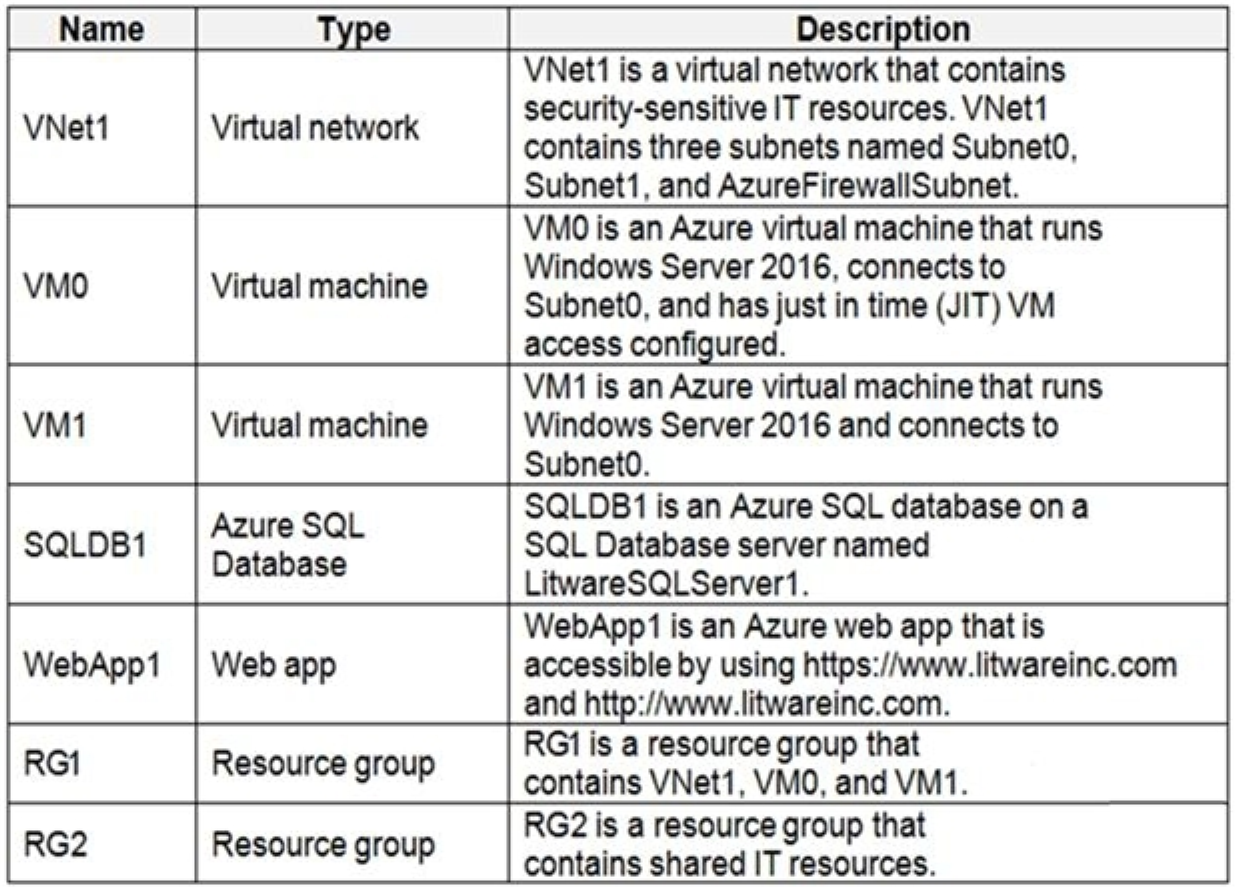
Sub1 is associated to an Azure Active Directory (Azure AD) tenant named litwareinc.com. The tenant contains the user objects and the device objects of all the Litware employees and their devices. Each user is assigned an Azure AD Premium P2 license. Azure AD Privileged Identity Management (PIM) is activated.

The tenant contains the groups shown in the following table.



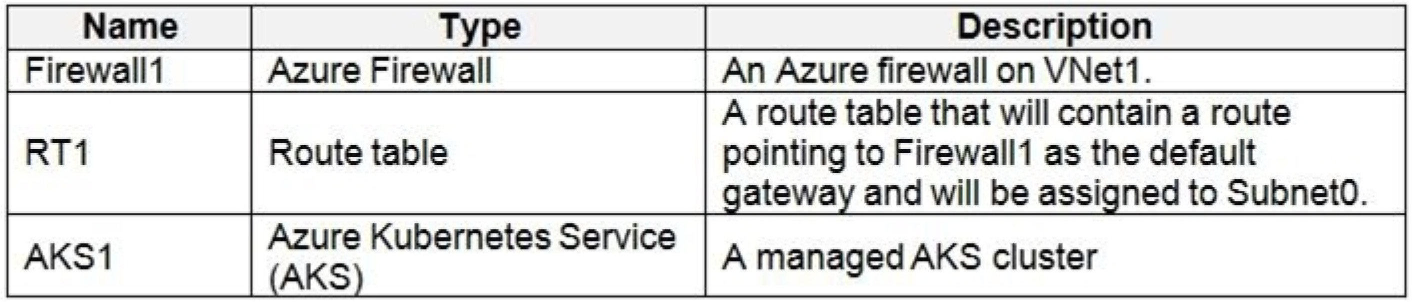
Name	Type	Description
Group1	Security group	A group that has the Dynamic User membership type, contains all the San Francisco users, and provides access to many Azure AD applications and Azure resources.
Group2	Security group	A group that has the Dynamic User membership type and contains the Chicago IT team

The Azure subscription contains the objects shown in the following table.



Name	Type	Description
VNet1	Virtual network	VNet1 is a virtual network that contains security-sensitive IT resources. VNet1 contains three subnets named Subnet0, Subnet1, and AzureFirewallSubnet.
VM0	Virtual machine	VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured.
VM1	Virtual machine	VM1 is an Azure virtual machine that runs Windows Server 2016 and connects to Subnet0.
SQLDB1	Azure SQL Database	SQLDB1 is an Azure SQL database on a SQL Database server named LitwareSQLServer1.
WebApp1	Web app	WebApp1 is an Azure web app that is accessible by using https://www.litwareinc.com and http://www.litwareinc.com.
RG1	Resource group	RG1 is a resource group that contains VNet1, VM0, and VM1.
RG2	Resource group	RG2 is a resource group that contains shared IT resources.

Identity and Access Requirements
Azure Security Center is set to the Standard tier.
Requirements
Planned Changes
Litware plans to deploy the Azure resources shown in the following table.



Name	Type	Description
Firewall1	Azure Firewall	An Azure firewall on VNet1.
RT1	Route table	A route table that will contain a route pointing to Firewall1 as the default gateway and will be assigned to Subnet0.
AKS1	Azure Kubernetes Service (AKS)	A managed AKS cluster

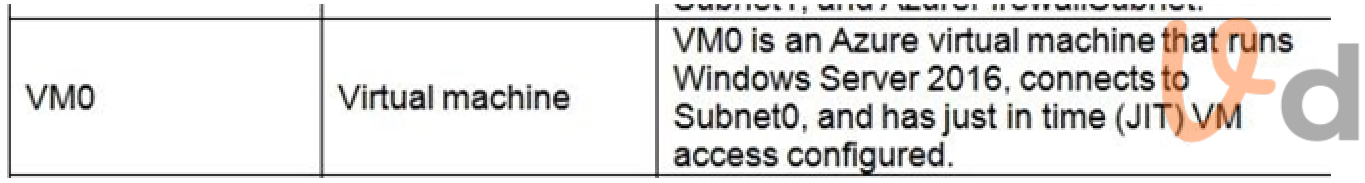
Litware identifies the following identity and access requirements:
All San Francisco users and their devices must be members of Group1.
The members of Group2 must be assigned the Contributor role to RG2 by using a permanent eligible assignment. Users must be prevented from registering applications in Azure AD and from consenting to applications that access company information on the users' behalf.
Platform Protection Requirements
Litware identifies the following platform protection requirements:
Microsoft Antimalware must be installed on the virtual machines in RG1.
The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role.
Azure AD users must be able to authenticate to AKS1 by using their Azure AD credentials.
Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access. A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in RG1. Role1 must be available only for RG1.
Security Operations Requirements
Litware must be able to customize the operating system security configurations in Azure Security Center. Data and Application Requirements
Litware identifies the following data and applications requirements:
The users in Group2 must be able to authenticate to SQLDB1 by using their Azure AD credentials.
WebApp1 must enforce mutual authentication.

General Requirements
Litware identifies the following general requirements:
Whenever possible, administrative effort must be minimized.
Whenever possible, use of automation must be maximized.

QUESTION 1
You need to ensure that users can access VM0. The solution must meet the platform protection requirements. What should you do?

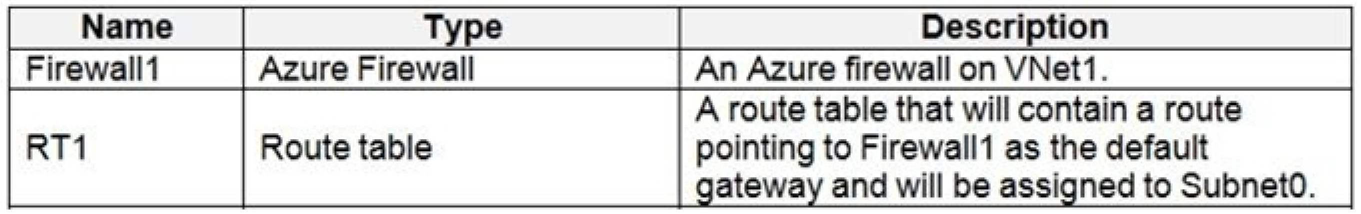
A. Move VM0 to Subnet1.
B. On Firewall, configure a network traffic filtering rule.
C. Assign RT1 to AzureFirewallSubnet.
D. On Firewall, configure a DNAT rule.

Correct Answer: A
Section:
Explanation:
Azure Firewall has the following known issue:
Conflict with Azure Security Center (ASC) Just-in-Time (JIT) feature.
If a virtual machine is accessed using JIT, and is in a subnet with a user-defined route that points to Azure Firewall as a default gateway, ASC JIT doesn't work. This is a result of asymmetric routing – a packet comes in via the virtual machine public IP (JIT opened the access), but the return path is via the firewall, which drops the packet because there is no established session on the firewall.
Solution: To work around this issue, place the JIT virtual machines on a separate subnet that doesn't have a user-defined route to the firewall.
Scenario:



		Subnet1, and AzureFirewallSubnet.
VM0	Virtual machine	VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured.

Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access.

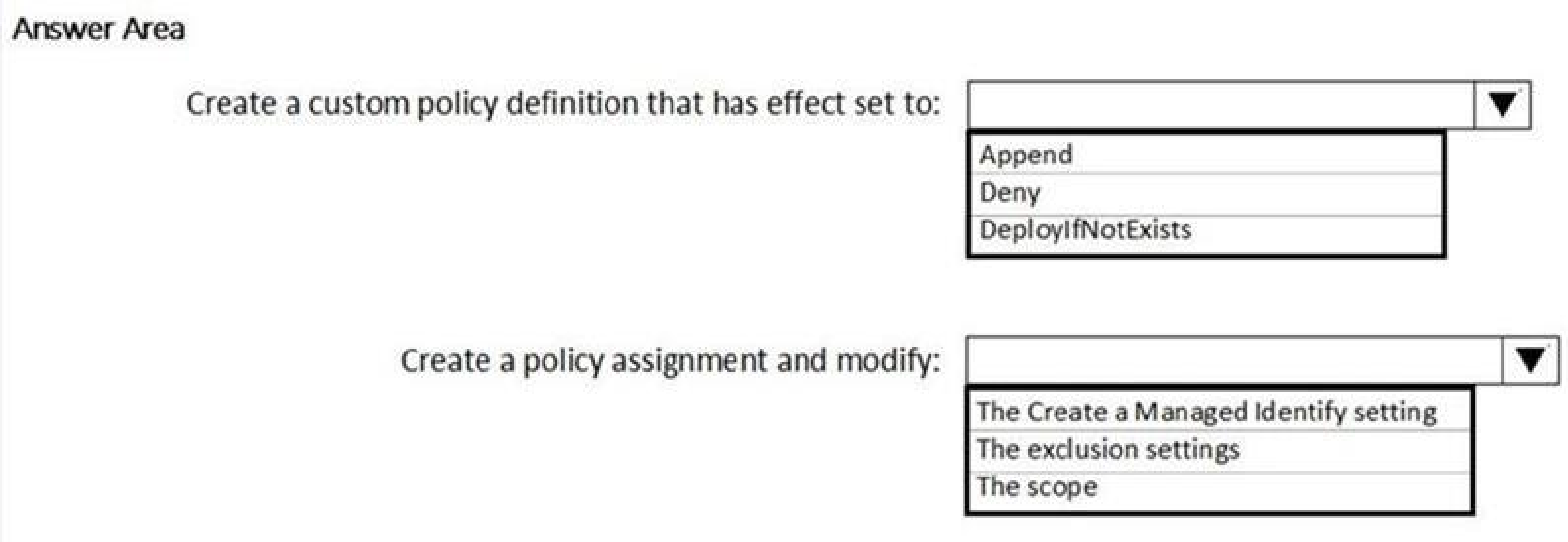


Name	Type	Description
Firewall1	Azure Firewall	An Azure firewall on VNet1.
RT1	Route table	A route table that will contain a route pointing to Firewall1 as the default gateway and will be assigned to Subnet0.

References:
https://docs.microsoft.com/en-us/azure/firewall/overview

QUESTION 2
HOTSPOT
You need to deploy Microsoft Antimalware to meet the platform protection requirements.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

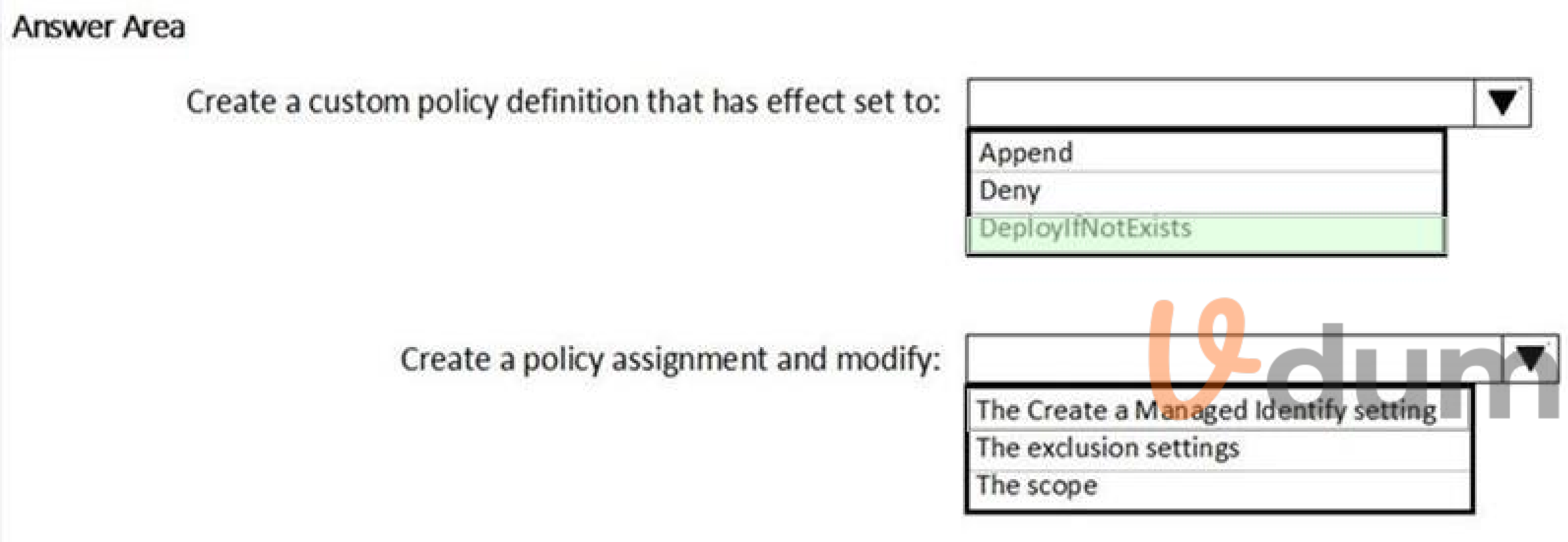
Create a custom policy definition that has effect set to:

- Append
- Deny
- DeployIfNotExists

Create a policy assignment and modify:

- The Create a Managed Identify setting
- The exclusion settings
- The scope

Answer Area:



Answer Area

Create a custom policy definition that has effect set to:

- Append
- Deny
- [✓ DeployIfNotExists]

Create a policy assignment and modify:

- The Create a Managed Identify setting
- The exclusion settings
- The scope

Section:

Explanation:

Scenario: Microsoft Antimalware must be installed on the virtual machines in RG1.

RG1 is a resource group that contains Vnet1, VM0, and VM1.

Box 1: DeployIfNotExists

DeployIfNotExists executes a template deployment when the condition is met.

Azure policy definition Antimalware

Incorrect Answers:

Append:

Append is used to add additional fields to the requested resource during creation or update. A common example is adding tags on resources such as costCenter or specifying allowed IPs for a storage resource.

Deny:

Deny is used to prevent a resource request that doesn't match defined standards through a policy definition and fails the request.

Box 2: The Create a Managed Identity setting

When Azure Policy runs the template in the deployIfNotExists policy definition, it does so using a managed identity. Azure Policy creates a managed identity for each assignment, but must have details about what roles to grant the managed identity.

Reference:

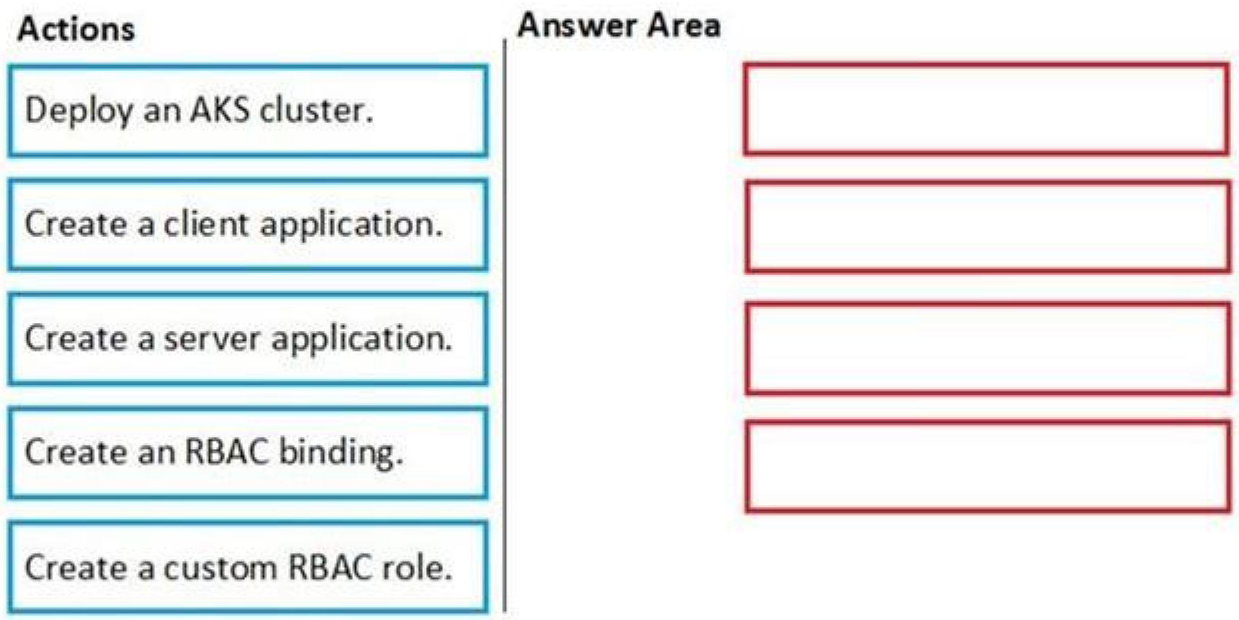
https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects

QUESTION 3

DRAG DROP

You need to deploy AKS1 to meet the platform protection requirements.
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.
NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.

Select and Place:



Actions

Deploy an AKS cluster.

Create a client application.

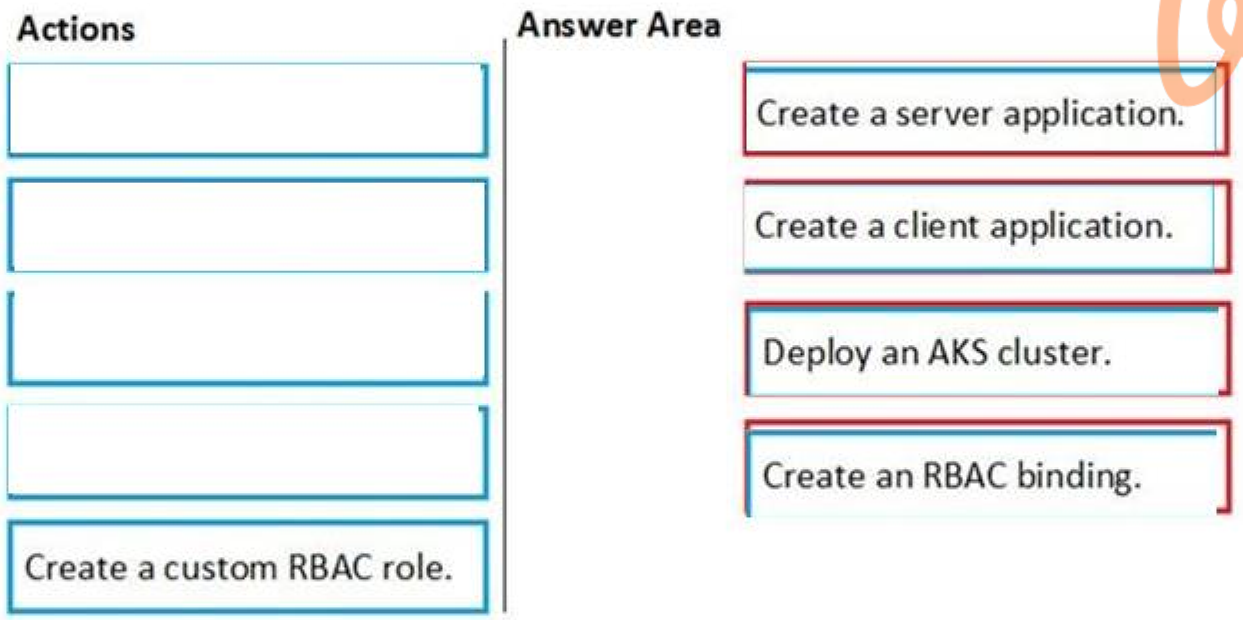
Create a server application.

Create an RBAC binding.

Create a custom RBAC role.

Answer Area

Correct Answer:



Actions

Create a custom RBAC role.

Answer Area

Create a server application.

Create a client application.

Deploy an AKS cluster.

Create an RBAC binding.

Section:
Explanation:
Scenario: Azure AD users must be to authenticate to AKS1 by using their Azure AD credentials.
Litewire plans to deploy AKS1, which is a managed AKS (Azure Kubernetes Services) cluster.
Step 1: Create a server application
To provide Azure AD authentication for an AKS cluster, two Azure AD applications are created. The first application is a server component that provides user authentication.
Step 2: Create a client application
The second application is a client component that's used when you're prompted by the CLI for authentication. This client application uses the server application for the actual authentication of the credentials provided by the client.
Step 3: Deploy an AKS cluster.

Use the az group create command to create a resource group for the AKS cluster.
Use the az aks create command to deploy the AKS cluster.
Step 4: Create an RBAC binding.
Before you use an Azure Active Directory account with an AKS cluster, you must create role-binding or cluster role-binding. Roles define the permissions to grant, and bindings apply them to desired users. These assignments can be applied to a given namespace, or across the entire cluster.
Reference:
https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration

03 - Implement platform protection

Case Study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

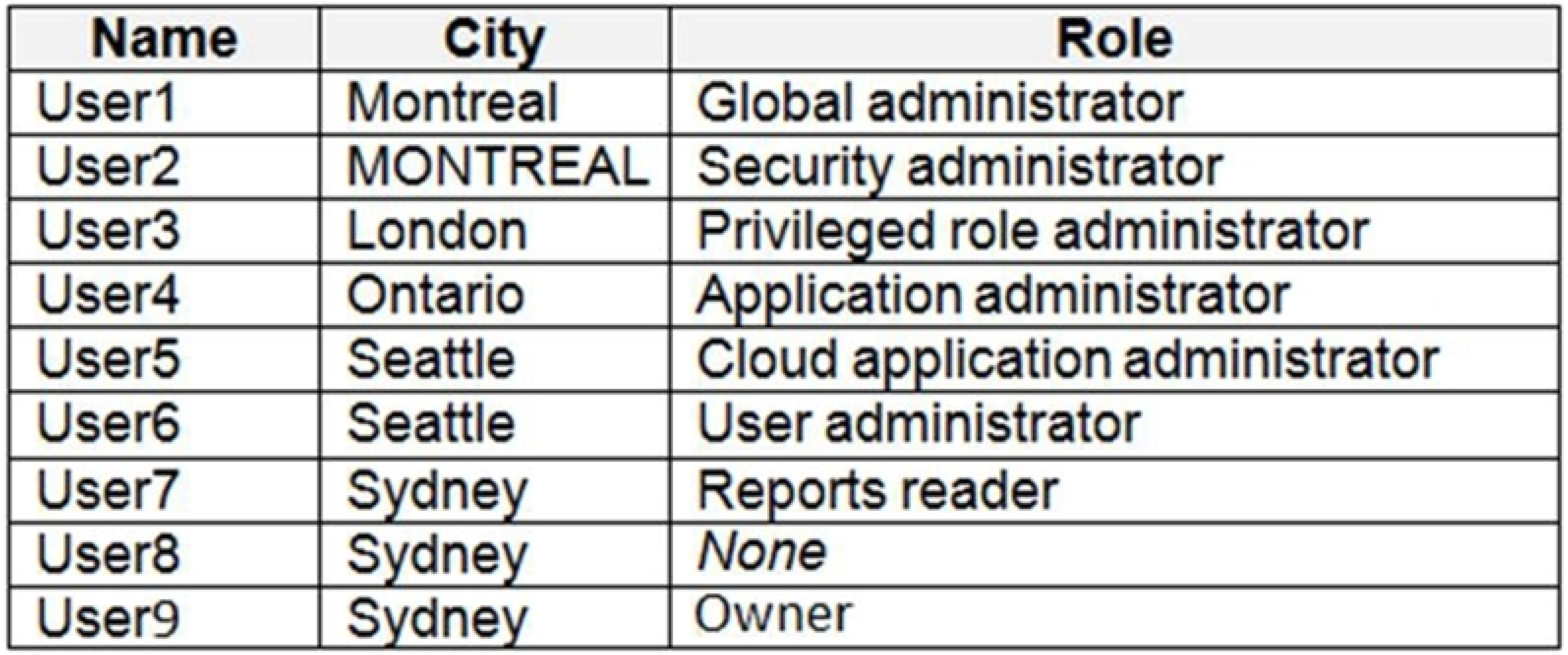
The company hosts its entire server infrastructure in Azure.

Contoso has two Azure subscriptions named Sub1 and Sub2. Both subscriptions are associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

Existing Environment

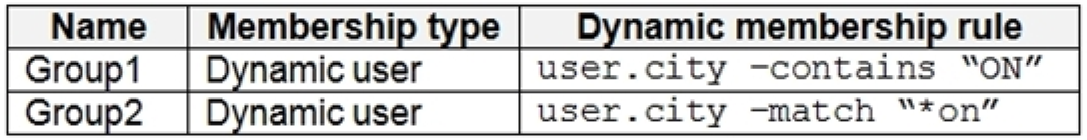
Azure AD

Contoso.com contains the users shown in the following table.



Name	City	Role
User1	Montreal	Global administrator
User2	MONTREAL	Security administrator
User3	London	Privileged role administrator
User4	Ontario	Application administrator
User5	Seattle	Cloud application administrator
User6	Seattle	User administrator
User7	Sydney	Reports reader
User8	Sydney	*None*
User9	Sydney	Owner

Contoso.com contains the security groups shown in the following table.

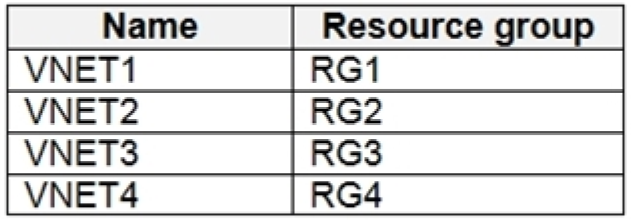


Name	Membership type	Dynamic membership rule
Group1	Dynamic user	`user.city -contains “ON”`
Group2	Dynamic user	`user.city -match “*on”`

Sub1

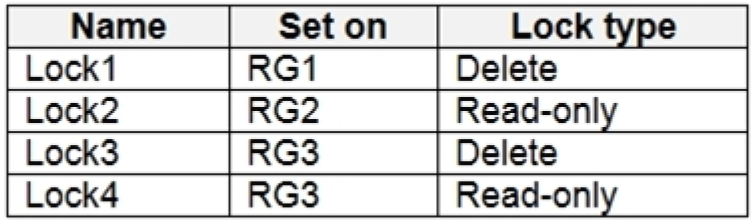
Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6.

User9 creates the virtual networks shown in the following table.



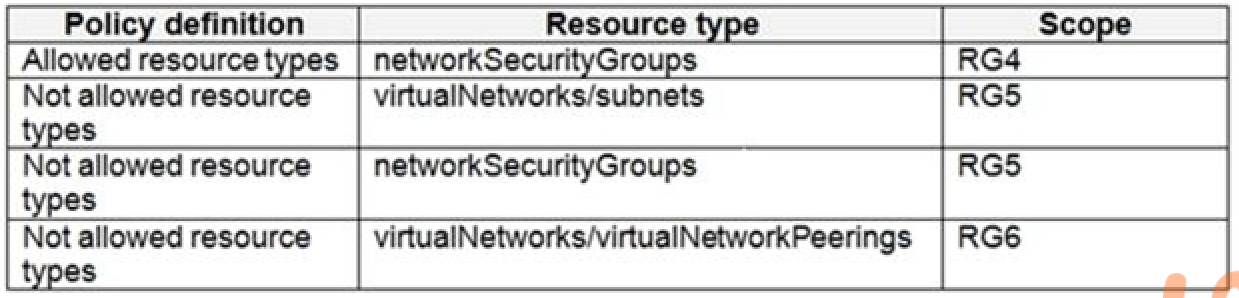
Name	Resource group
VNET1	RG1
VNET2	RG2
VNET3	RG3
VNET4	RG4

Sub1 contains the locks shown in the following table.



Name	Set on	Lock type
Lock1	RG1	Delete
Lock2	RG2	Read-only
Lock3	RG3	Delete
Lock4	RG3	Read-only

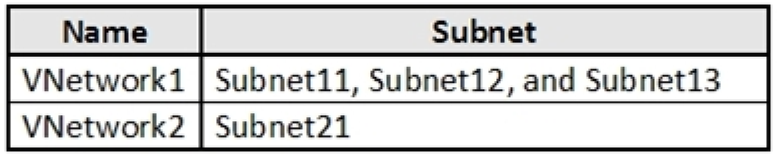
Sub1 contains the Azure policies shown in the following table.



Policy definition	Resource type	Scope
Allowed resource types	networkSecurityGroups	RG4
Not allowed resource types	virtualNetworks/subnets	RG5
Not allowed resource types	networkSecurityGroups	RG5
Not allowed resource types	virtualNetworks/virtualNetworkPeerings	RG6

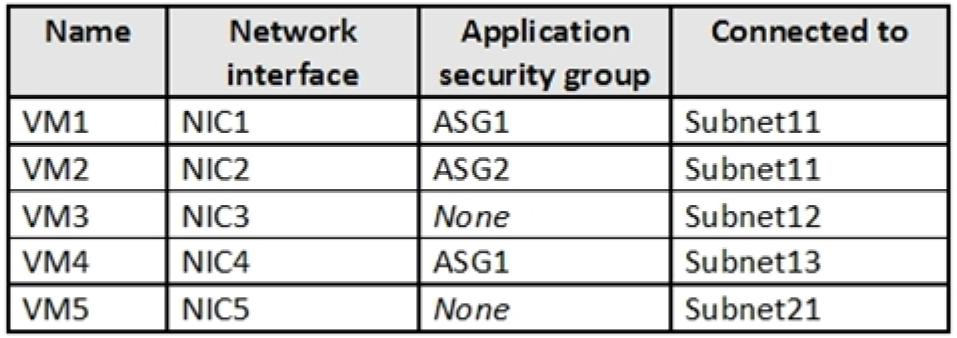
Sub2

Sub2 contains the virtual networks shown in the following table.



Name	Subnet
VNetwork1	Subnet11, Subnet12, and Subnet13
VNetwork2	Subnet21

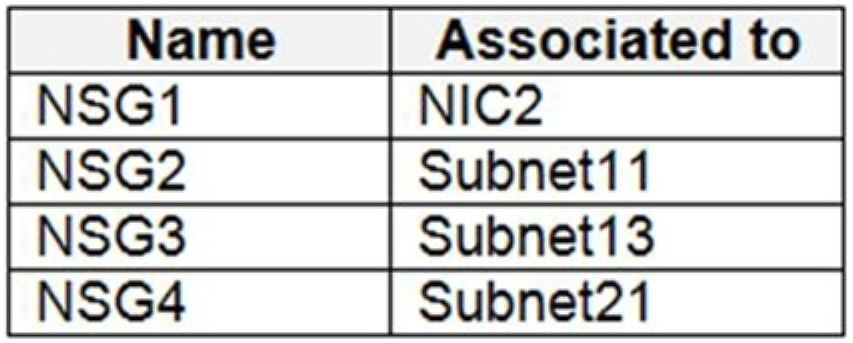
Sub2 contains the virtual machines shown in the following table.



Name	Network interface	Application security group	Connected to
VM1	NIC1	ASG1	Subnet11
VM2	NIC2	ASG2	Subnet11
VM3	NIC3	*None*	Subnet12
VM4	NIC4	ASG1	Subnet13
VM5	NIC5	*None*	Subnet21

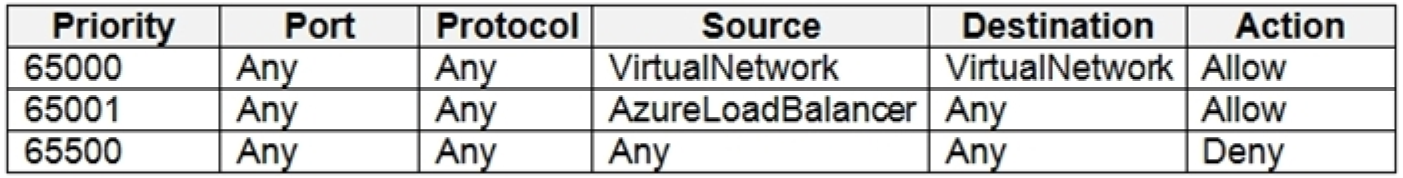
All virtual machines have public IP addresses and the Web Server (IIS) role installed. The firewalls for each virtual machine allow ping requests and web requests.

Sub2 contains the network security groups (NSGs) shown in the following table.



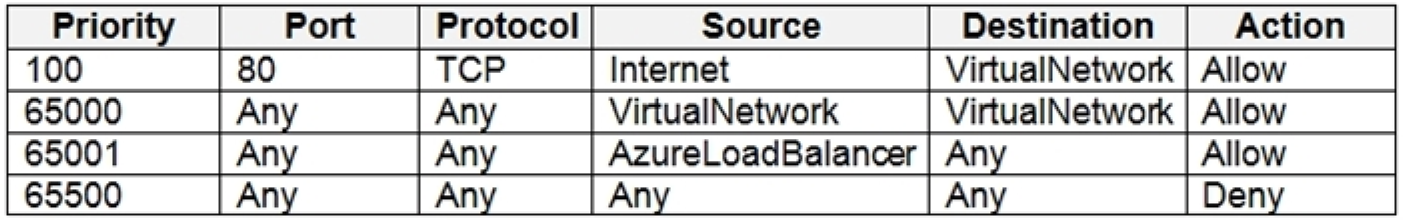
Name	Associated to
NSG1	NIC2
NSG2	Subnet11
NSG3	Subnet13
NSG4	Subnet21

NSG1 has the inbound security rules shown in the following table.



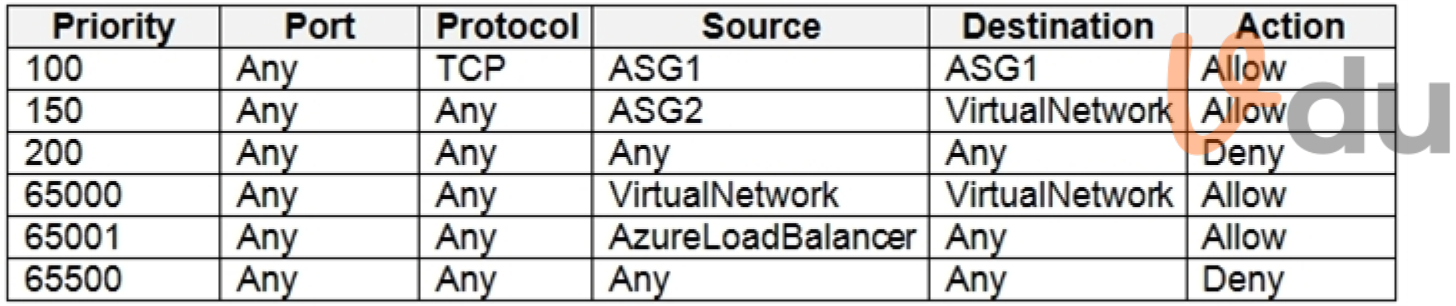
Priority	Port	Protocol	Source	Destination	Action
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG2 has the inbound security rules shown in the following table.



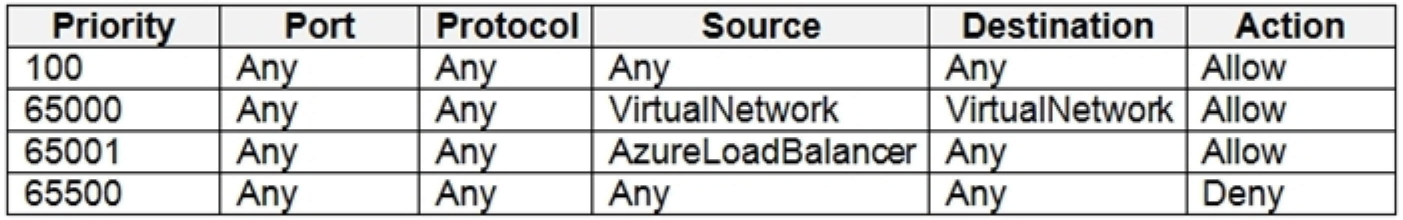
Priority	Port	Protocol	Source	Destination	Action
100	80	TCP	Internet	VirtualNetwork	Allow
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG3 has the inbound security rules shown in the following table.



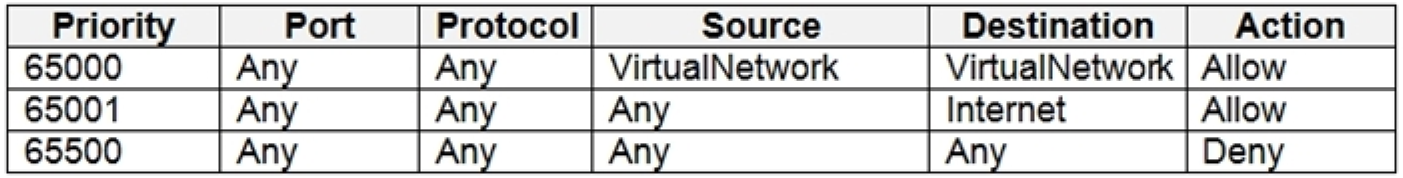
Priority	Port	Protocol	Source	Destination	Action
100	Any	TCP	ASG1	ASG1	Allow
150	Any	Any	ASG2	VirtualNetwork	Allow
200	Any	Any	Any	Any	Deny
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG4 has the inbound security rules shown in the following table.



Priority	Port	Protocol	Source	Destination	Action
100	Any	Any	Any	Any	Allow
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG1, NSG2, NSG3, and NSG4 have the outbound security rules shown in the following table.



Priority	Port	Protocol	Source	Destination	Action
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	Any	Internet	Allow
65500	Any	Any	Any	Any	Deny

Technical requirements

Contoso identifies the following technical requirements:

Deploy Azure Firewall to VNetwork1 in Sub2.

Register an application named App2 in contoso.com.

Whenever possible, use the principle of least privilege.

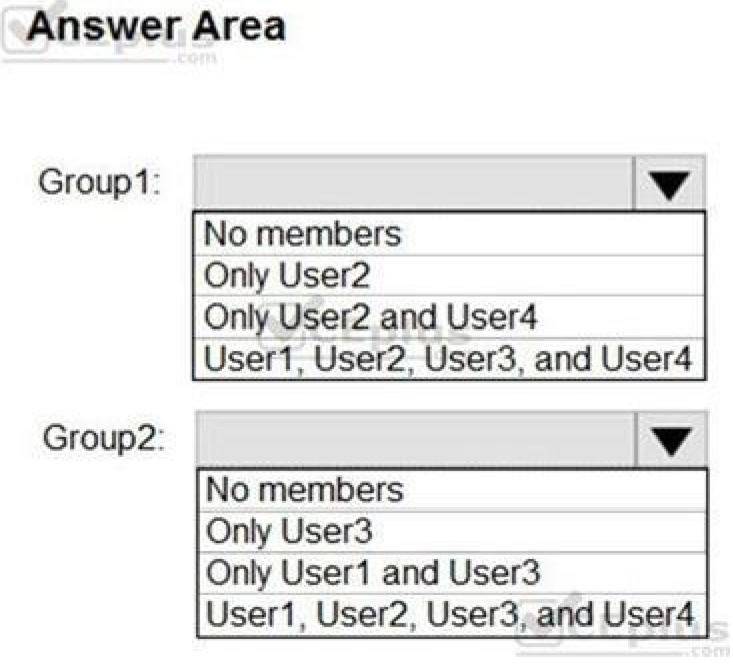
Enable Azure AD Privileged Identity Management (PIM) for contoso.com.

QUESTION 1

HOTSPOT

What is the membership of Group1 and Group2? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

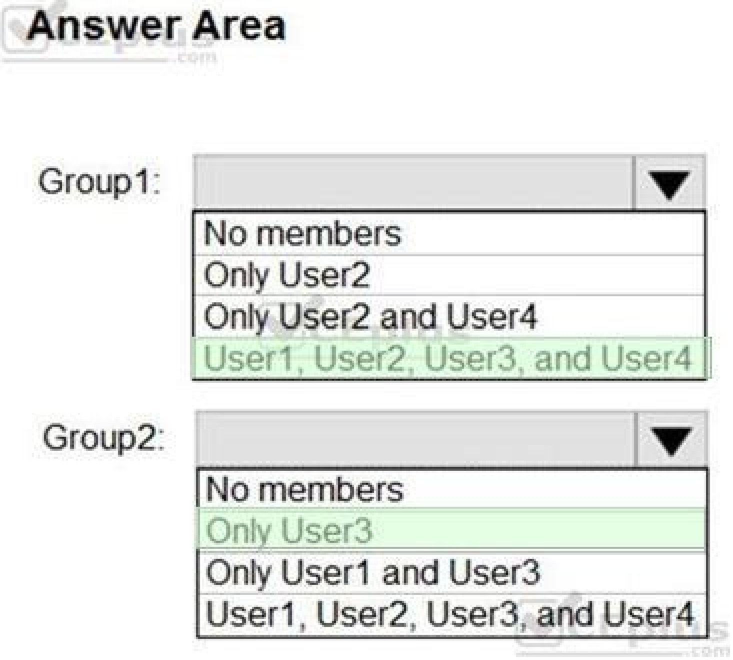


Answer Area

Group1:
- No members
- Only User2
- Only User2 and User4
- User1, User2, User3, and User4

Group2:
- No members
- Only User3
- Only User1 and User3
- User1, User2, User3, and User4

Answer Area:



Answer Area

Group1:
- No members
- Only User2
- Only User2 and User4
- [✓ User1, User2, User3, and User4]

Group2:
- No members
- [✓ Only User3]
- Only User1 and User3
- User1, User2, User3, and User4

Section:

Explanation:

Box 1: User1, User2, User3, User4

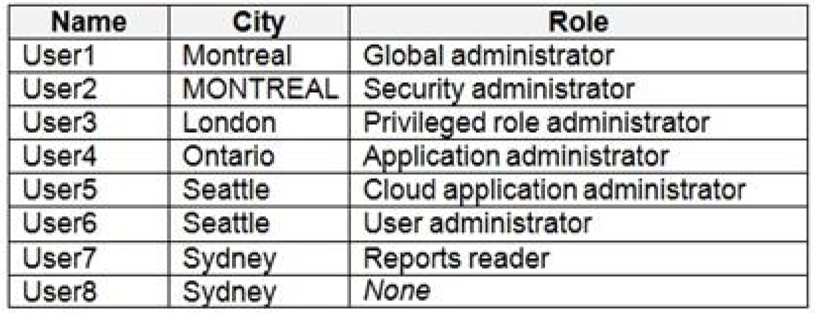
Contains "ON" is true for Montreal (User1), MONTREAL (User2), London (User 3), and Ontario (User4) as string and regex operations are not case sensitive.

Box 2: Only User3

Match "*on" is only true for London (User3).

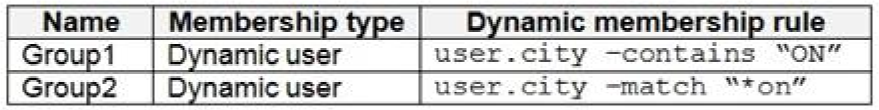
Scenario:

Contoso.com contains the users shown in the following table.



Name	City	Role
User1	Montreal	Global administrator
User2	MONTREAL	Security administrator
User3	London	Privileged role administrator
User4	Ontario	Application administrator
User5	Seattle	Cloud application administrator
User6	Seattle	User administrator
User7	Sydney	Reports reader
User8	Sydney	*None*

Contoso.com contains the security groups shown in the following table.



Name	Membership type	Dynamic membership rule
Group1	Dynamic user	`user.city -contains "ON"`
Group2	Dynamic user	`user.city -match "*on"`

References:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership

QUESTION 2

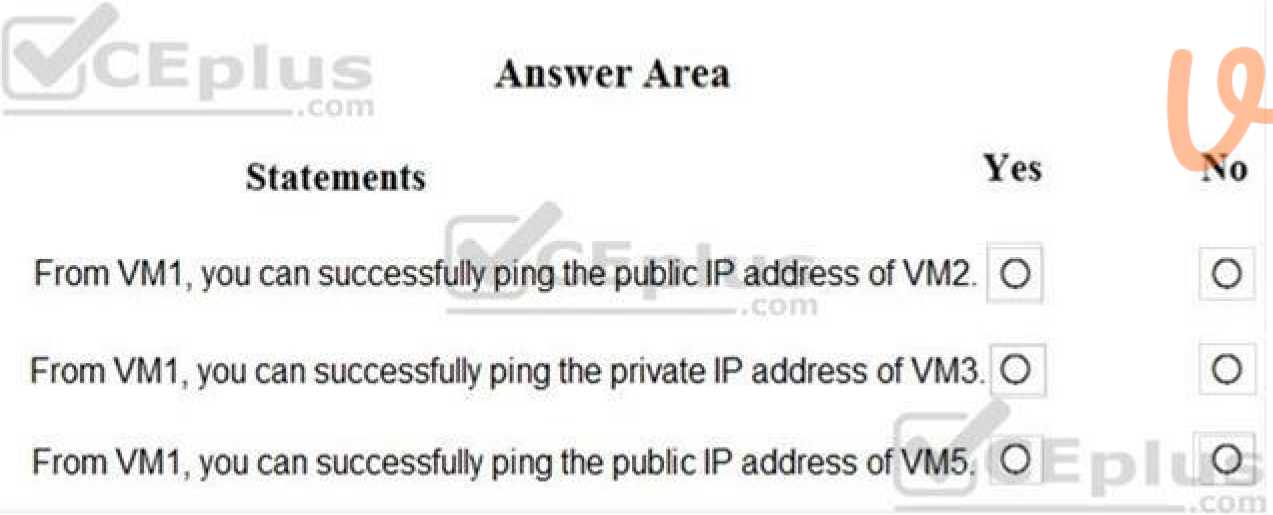
HOTSPOT

You are evaluating the security of the network communication between the virtual machines in Sub2.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

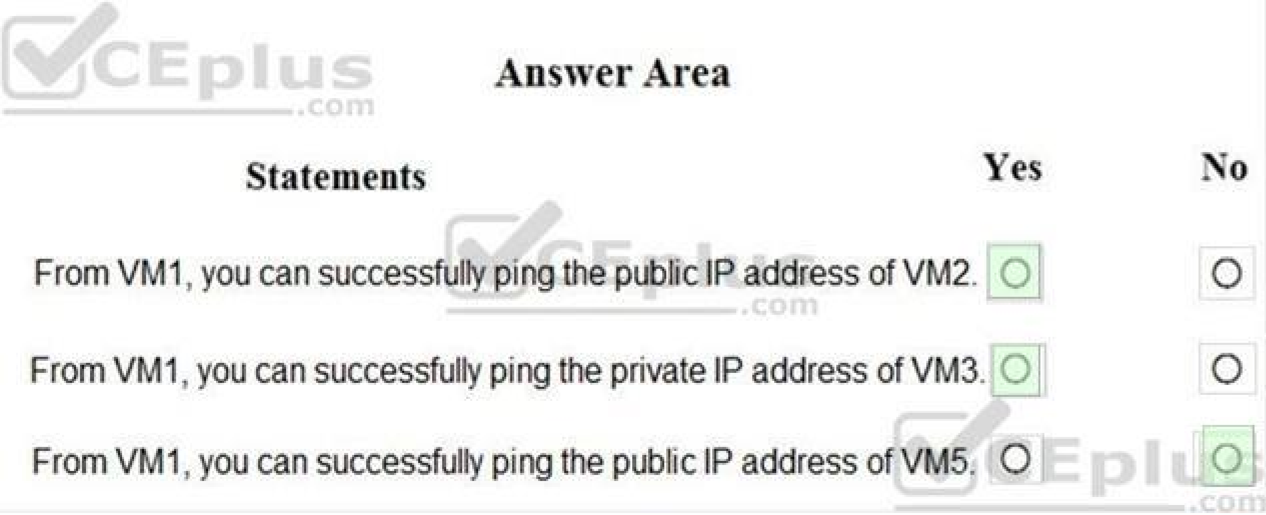
Hot Area:



Answer Area

Statements	Yes	No
From VM1, you can successfully ping the public IP address of VM2.	○	○
From VM1, you can successfully ping the private IP address of VM3.	○	○
From VM1, you can successfully ping the public IP address of VM5.	○	○

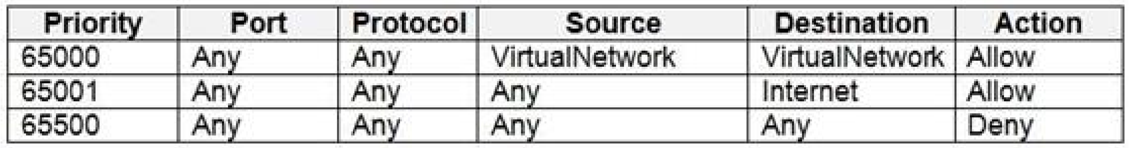
Answer Area:



Answer Area

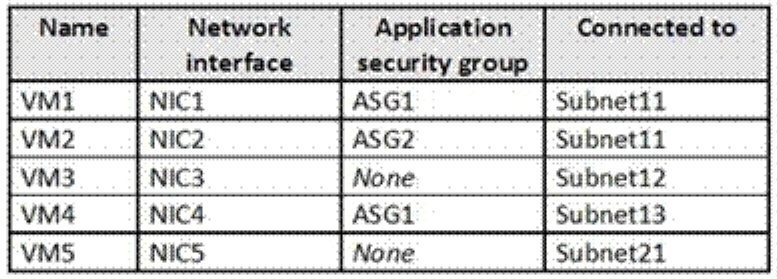
Statements	Yes	No
From VM1, you can successfully ping the public IP address of VM2.	[✓ ○]	○
From VM1, you can successfully ping the private IP address of VM3.	[✓ ○]	○
From VM1, you can successfully ping the public IP address of VM5.	○	[✓ ○]

Section:
Explanation:
Box 1: Yes. All traffic is allowed out to the Internet so you can ping the public IP.
NSG1, NSG2, NSG3, and NSG4 have the outbound security rules shown in the following table.

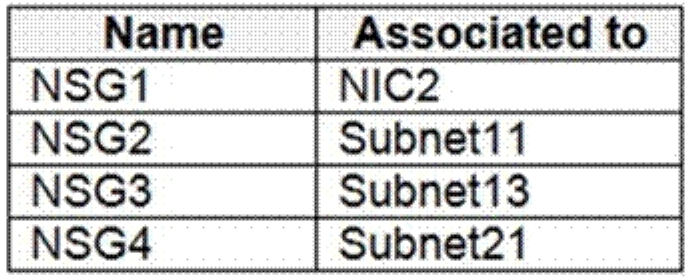


Priority	Port	Protocol	Source	Destination	Action
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	Any	Internet	Allow
65500	Any	Any	Any	Any	Deny

Box 2: Yes. VM3 is on Subnet12. There is no NSG attached to Subnet12 so the traffic will be allowed by default.

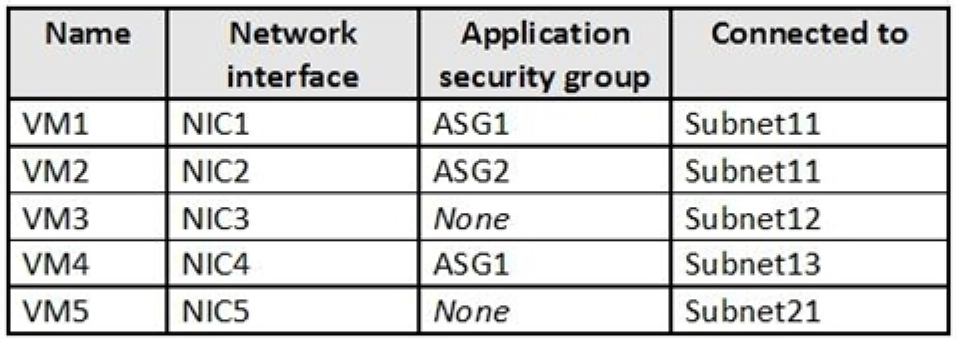


Name	Network interface	Application security group	Connected to
VM1	NIC1	ASG1	Subnet11
VM2	NIC2	ASG2	Subnet11
VM3	NIC3	*None*	Subnet12
VM4	NIC4	ASG1	Subnet13
VM5	NIC5	*None*	Subnet21

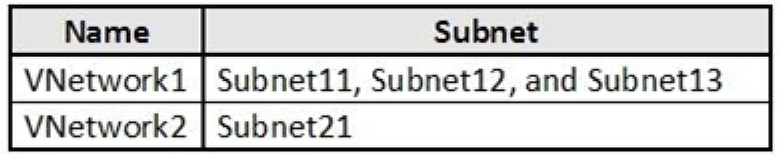


Name	Associated to
NSG1	NIC2
NSG2	Subnet11
NSG3	Subnet13
NSG4	Subnet21

Box 3: No (because VM5 is in a separate VNet).
Note: Sub2 contains the virtual machines shown in the following table.



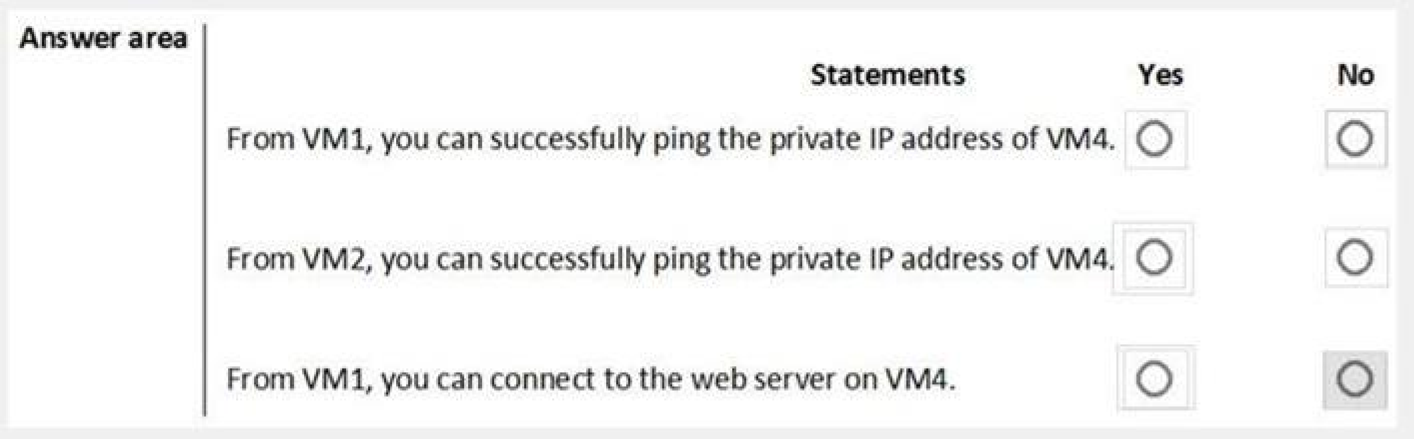
Name	Network interface	Application security group	Connected to
VM1	NIC1	ASG1	Subnet11
VM2	NIC2	ASG2	Subnet11
VM3	NIC3	*None*	Subnet12
VM4	NIC4	ASG1	Subnet13
VM5	NIC5	*None*	Subnet21



Name	Subnet
VNetwork1	Subnet11, Subnet12, and Subnet13
VNetwork2	Subnet21

QUESTION 3
HOTSPOT
You are evaluating the effect of the application security groups on the network communication between the virtual machines in Sub2.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

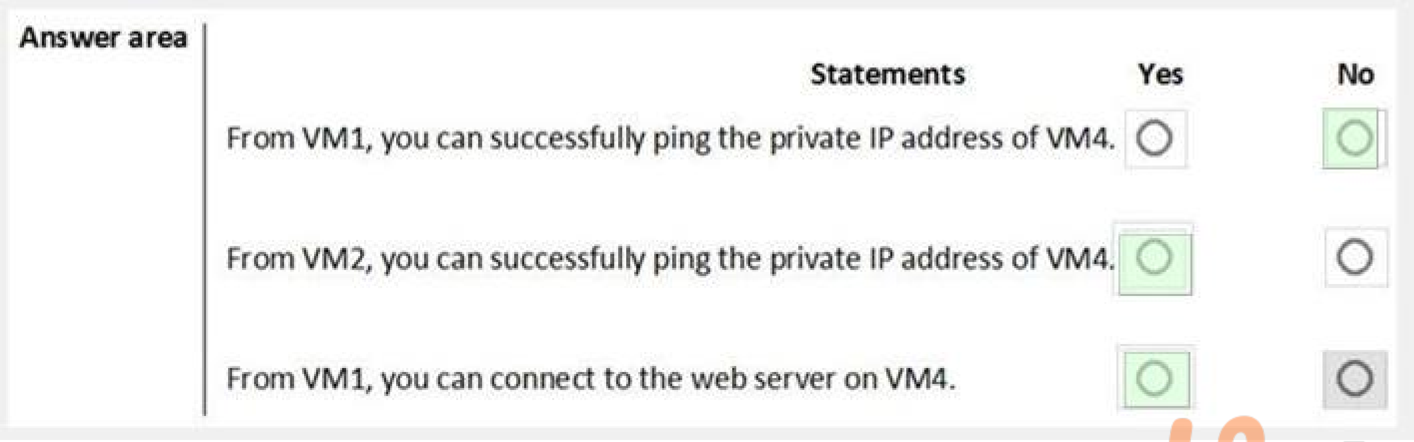
Hot Area:



Answer area

Statements	Yes	No
From VM1, you can successfully ping the private IP address of VM4.	○	○
From VM2, you can successfully ping the private IP address of VM4.	○	○
From VM1, you can connect to the web server on VM4.	○	○

Answer Area:



Answer area

Statements	Yes	No
From VM1, you can successfully ping the private IP address of VM4.	○	[✓ ○]
From VM2, you can successfully ping the private IP address of VM4.	[✓ ○]	○
From VM1, you can connect to the web server on VM4.	[✓ ○]	○

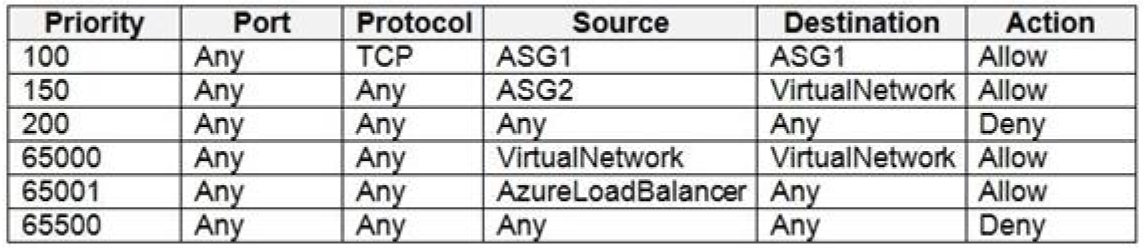
Section:

Explanation:

Box 1: No. VM4 is in Subnet13 which has NSG3 attached to it.

VM1 is in ASG1. NSG3 would only allow ICMP pings from ASG2 but not ASG1. Only TCP traffic is allowed from ASG1.

NSG3 has the inbound security rules shown in the following table.



Priority	Port	Protocol	Source	Destination	Action
100	Any	TCP	ASG1	ASG1	Allow
150	Any	Any	ASG2	VirtualNetwork	Allow
200	Any	Any	Any	Any	Deny
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

Box 2: Yes.

VM2 is in ASG2. Any protocol is allowed from ASG2 so ICMP ping would be allowed.

Box3. VM1 is in ASG1. TCP traffic is allowed from ASG1 so VM1 could connect to the web server as connections to the web server would be on ports TCP 80 or TCP 443.

QUESTION 4

You need to meet the technical requirements for VNetwork1.

What should you do first?

A. Create a new subnet on VNetwork1.

B. Remove the NSGs from Subnet11 and Subnet13.

C. Associate an NSG to Subnet12.

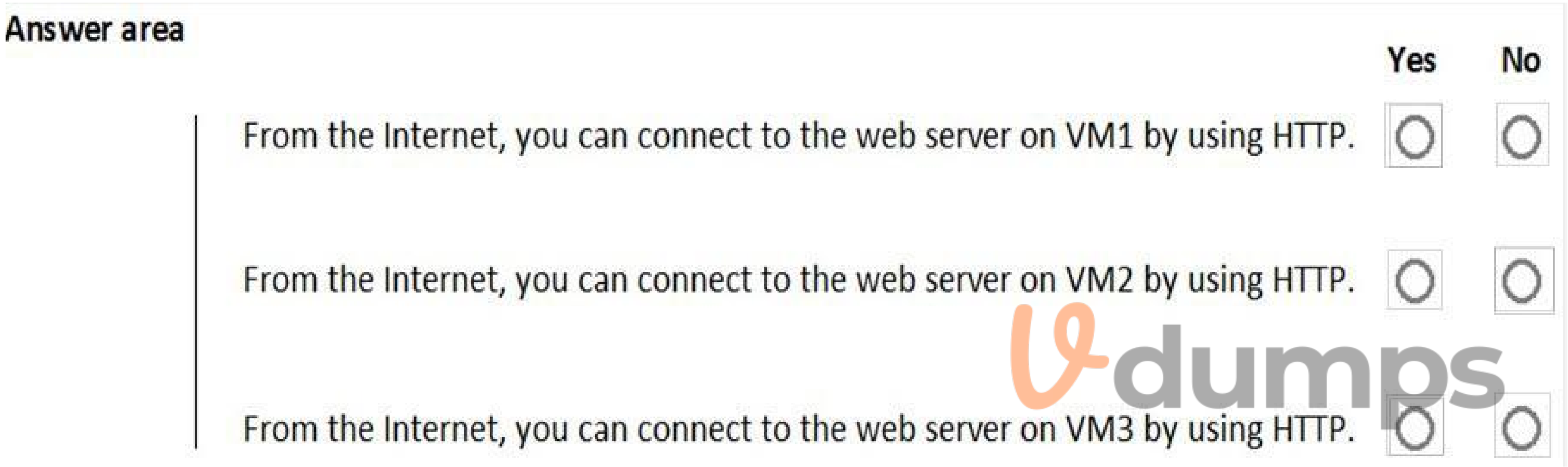
D. Configure DDoS protection for VNetwork1.

Correct Answer: A

Section:
Explanation:
From scenario: Deploy Azure Firewall to VNetwork1 in Sub2.
Azure firewall needs a dedicated subnet named AzureFirewallSubnet.
References:
https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal

QUESTION 5
HOTSPOT
You are evaluating the security of VM1, VM2, and VM3 in Sub2.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

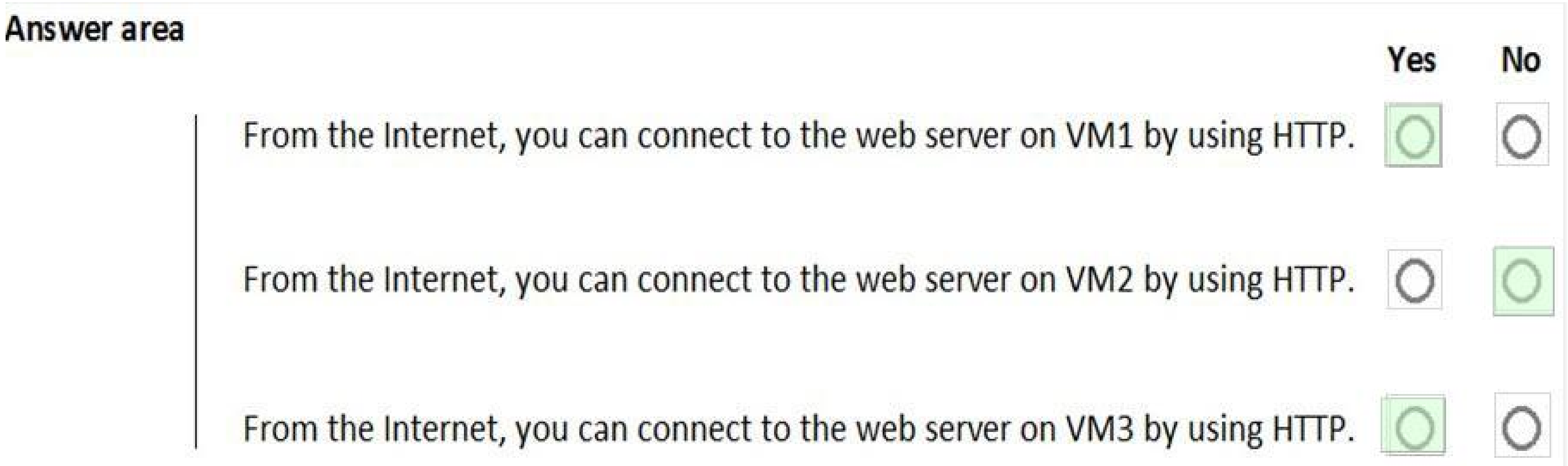
Hot Area:



Answer area

	Yes	No
From the Internet, you can connect to the web server on VM1 by using HTTP.	○	○
From the Internet, you can connect to the web server on VM2 by using HTTP.	○	○
From the Internet, you can connect to the web server on VM3 by using HTTP.	○	○

Answer Area:



Answer area

	Yes	No
From the Internet, you can connect to the web server on VM1 by using HTTP.	[✓ ○]	○
From the Internet, you can connect to the web server on VM2 by using HTTP.	○	[✓ ○]
From the Internet, you can connect to the web server on VM3 by using HTTP.	[✓ ○]	○

Section:
Explanation:
VM1: Yes. NSG2 applies to VM1 and this allows inbound traffic on port 80.
VM2: No. NSG2 and NSG1 apply to VM2. NSG2 allows the inbound traffic on port 80 but NSG1 does not allow it. VM3: Yes. There are no NSGs applying to VM3 so all ports will be open.

01 - Manage security operations

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

General Overview

Fabrikam, Inc. is a consulting company that has a main office in Montreal and branch offices in Seattle and New York. Fabrikam has IT, human resources (HR), and finance departments.

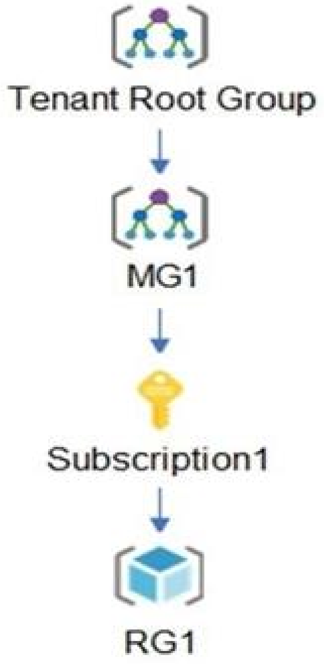
Existing Environment

Network Environment

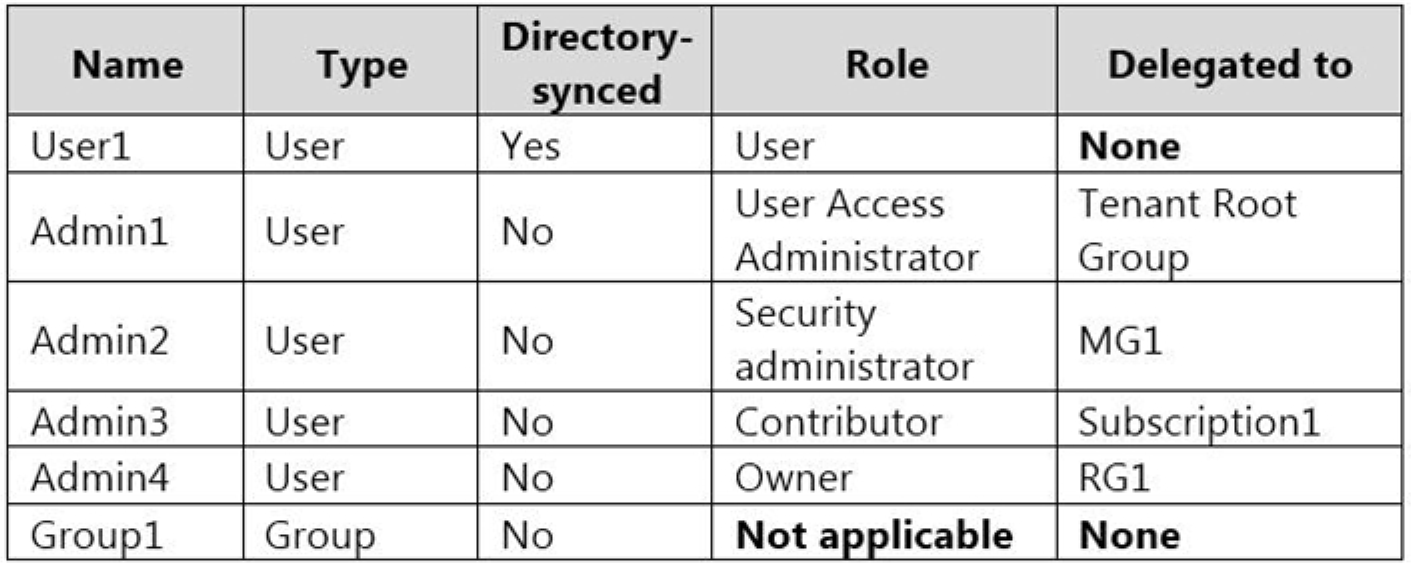
Fabrikam has a Microsoft 365 subscription and an Azure subscription named subscription1.

The network contains an on-premises Active Directory domain named Fabrikam.com. The domain contains two organizational units (OUs) named OU1 and OU2. Azure AD Connect cloud sync syncs only OU1.

The Azure resources hierarchy is shown in the following exhibit.

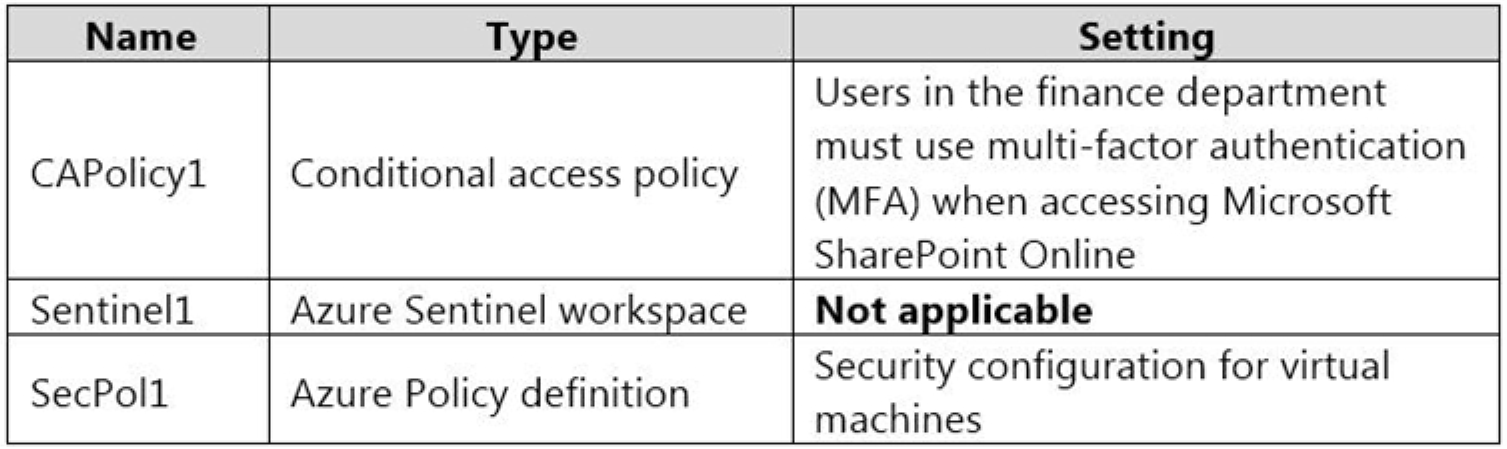


The Azure Active Directory (Azure AD) tenant contains the users shown in the following table.



Name	Type	Directory-synced	Role	Delegated to
User1	User	Yes	User	**None**
Admin1	User	No	User Access Administrator	Tenant Root Group
Admin2	User	No	Security administrator	MG1
Admin3	User	No	Contributor	Subscription1
Admin4	User	No	Owner	RG1
Group1	Group	No	**Not applicable**	**None**

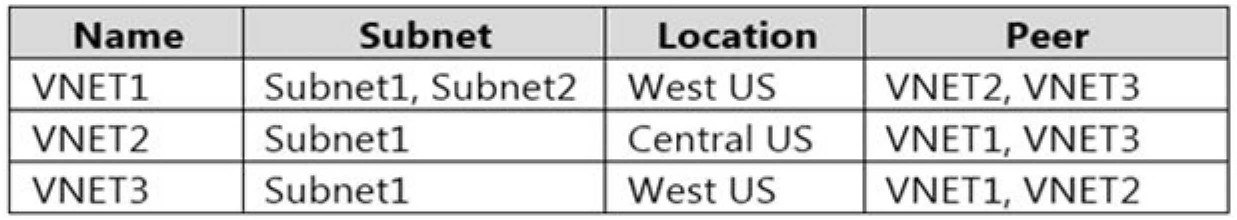
Azure AD contains the resources shown in the following table.



Name	Type	Setting
CAPolicy1	Conditional access policy	Users in the finance department must use multi-factor authentication (MFA) when accessing Microsoft SharePoint Online
Sentinel1	Azure Sentinel workspace	**Not applicable**
SecPol1	Azure Policy definition	Security configuration for virtual machines

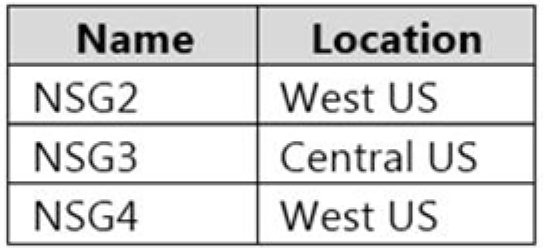
Subscription1 Resources

Subscription1 contains the virtual networks shown in the following table.



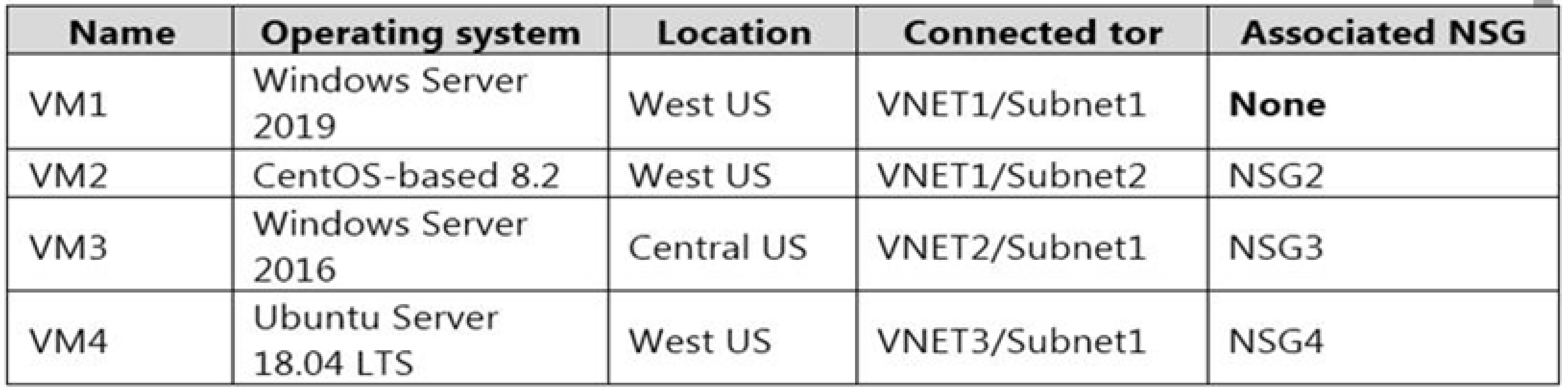
Name	Subnet	Location	Peer
VNET1	Subnet1, Subnet2	West US	VNET2, VNET3
VNET2	Subnet1	Central US	VNET1, VNET3
VNET3	Subnet1	West US	VNET1, VNET2

Subscription1 contains the network security groups (NSGs) shown in the following table.



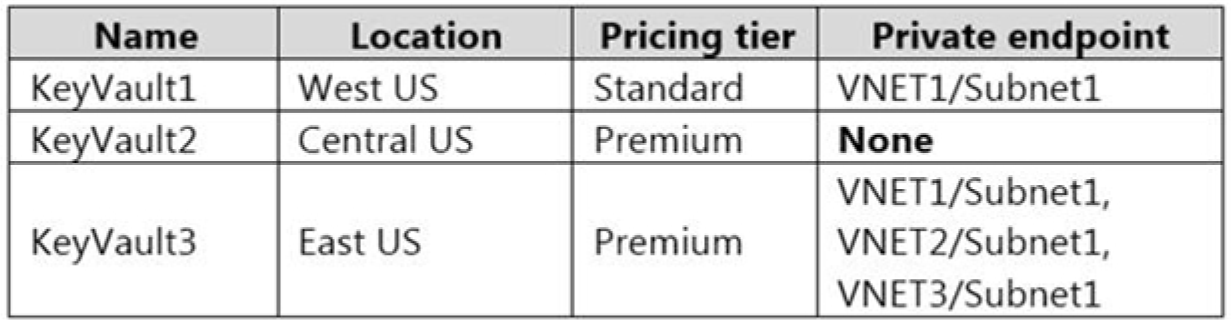
Name	Location
NSG2	West US
NSG3	Central US
NSG4	West US

Subscription1 contains the virtual machines shown in the following table.



Name	Operating system	Location	Connected tor	Associated NSG
VM1	Windows Server 2019	West US	VNET1/Subnet1	**None**
VM2	CentOS-based 8.2	West US	VNET1/Subnet2	NSG2
VM3	Windows Server 2016	Central US	VNET2/Subnet1	NSG3
VM4	Ubuntu Server 18.04 LTS	West US	VNET3/Subnet1	NSG4

Subscription1 contains the Azure key vaults shown in the following table.



Name	Location	Pricing tier	Private endpoint
KeyVault1	West US	Standard	VNET1/Subnet1
KeyVault2	Central US	Premium	**None**
KeyVault3	East US	Premium	VNET1/Subnet1, VNET2/Subnet1, VNET3/Subnet1

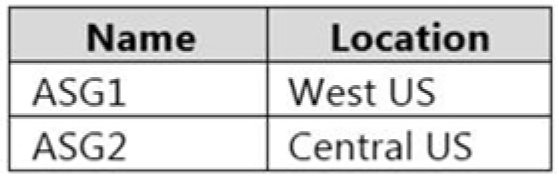
Subscription1 contains a storage account named storage1 in the West US Azure region.

Planned Changes and Requirements

Planned Changes

Fabrikam plans to implement the following changes:

Create two application security groups as shown in the following table.



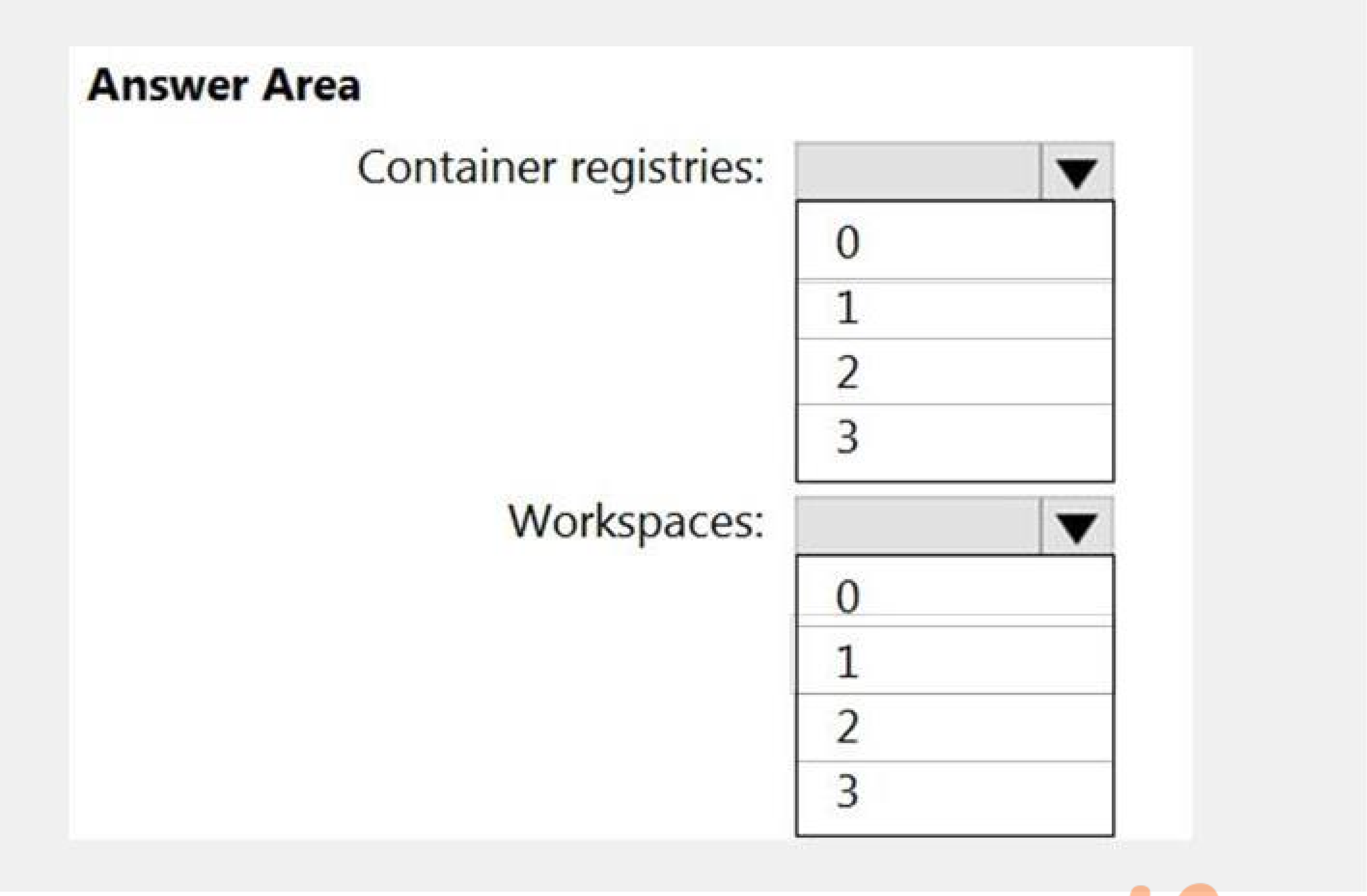
Name	Location
ASG1	West US
ASG2	Central US

Associate the network interface of VM1 to ASG1.
Deploy SecPol1 by using Azure Security Center.
Deploy a third-party app named App1. A version of App1 exists for all available operating systems.
Create a resource group named RG2.
Sync OU2 to Azure AD.
Add User1 to Group1.
Technical Requirements
Fabrikam identifies the following technical requirements:
The finance department users must reauthenticate after three hours when they access SharePoint Online. Storage1 must be encrypted by using customer-managed keys and automatic key rotation.
From Sentinel1, you must ensure that the following notebooks can be launched:
- Entity Explorer – Account
- Entity Explorer – Windows Host
- Guided Investigation Process Alerts
VM1, VM2, and VM3 must be encrypted by using Azure Disk Encryption.
Just in time (JIT) VM access for VM1, VM2, and VM3 must be enabled.
App1 must use a secure connection string stored in KeyVault1.
KeyVault1 traffic must NOT travel over the internet.

QUESTION 1

HOTSPOT
You need to configure support for Azure Sentinel notebooks to meet the technical requirements.
What is the minimum number of Azure container registries and Azure Machine Learning workspaces required?

Hot Area:

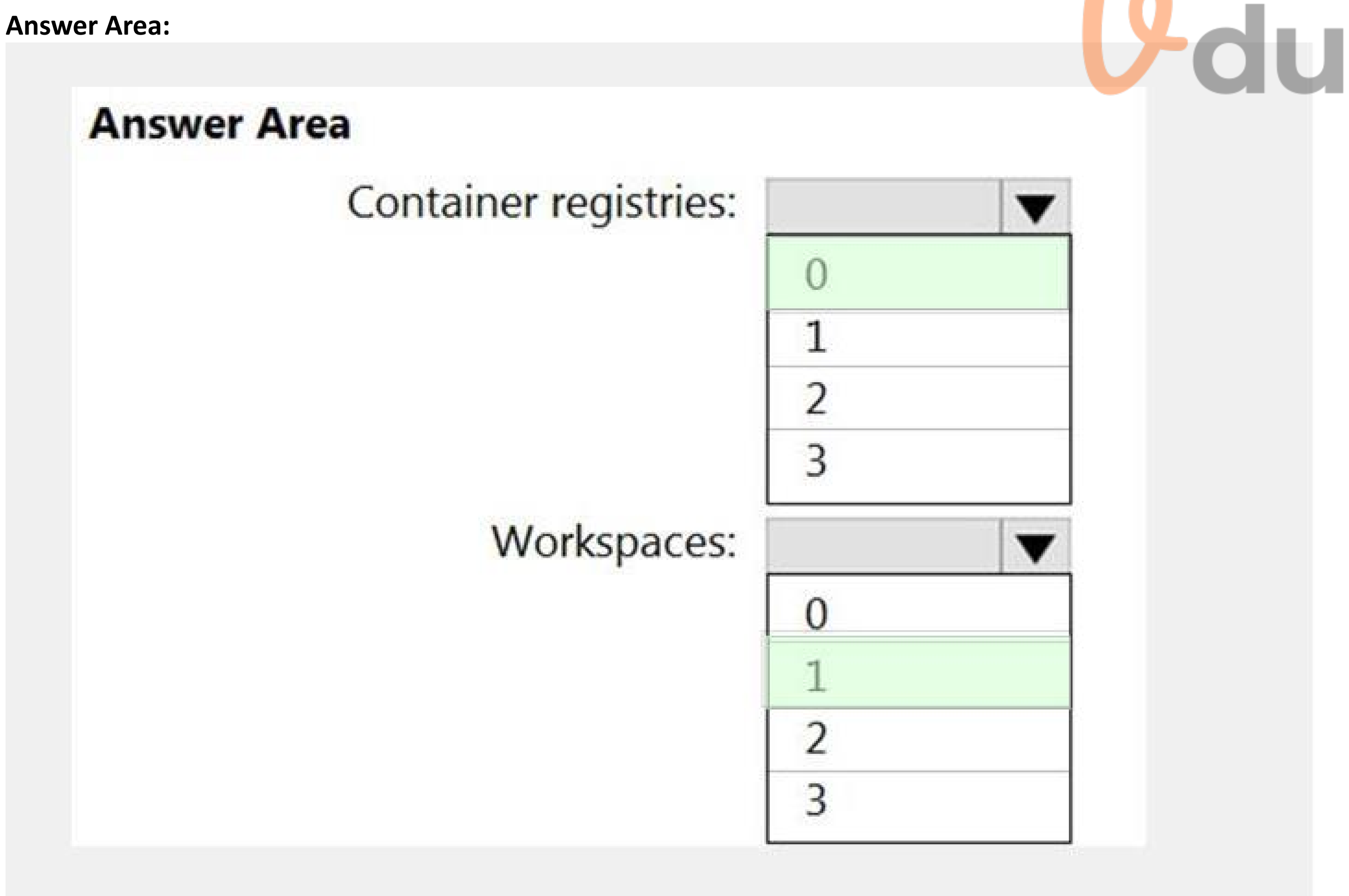


Answer Area

Container registries:
- 0
- 1
- 2
- 3

Workspaces:
- 0
- 1
- 2
- 3

Answer Area:



Answer Area

Container registries:
- [✓ 0]
- 1
- 2
- 3

Workspaces:
- 0
- [✓ 1]
- 2
- 3

Section:

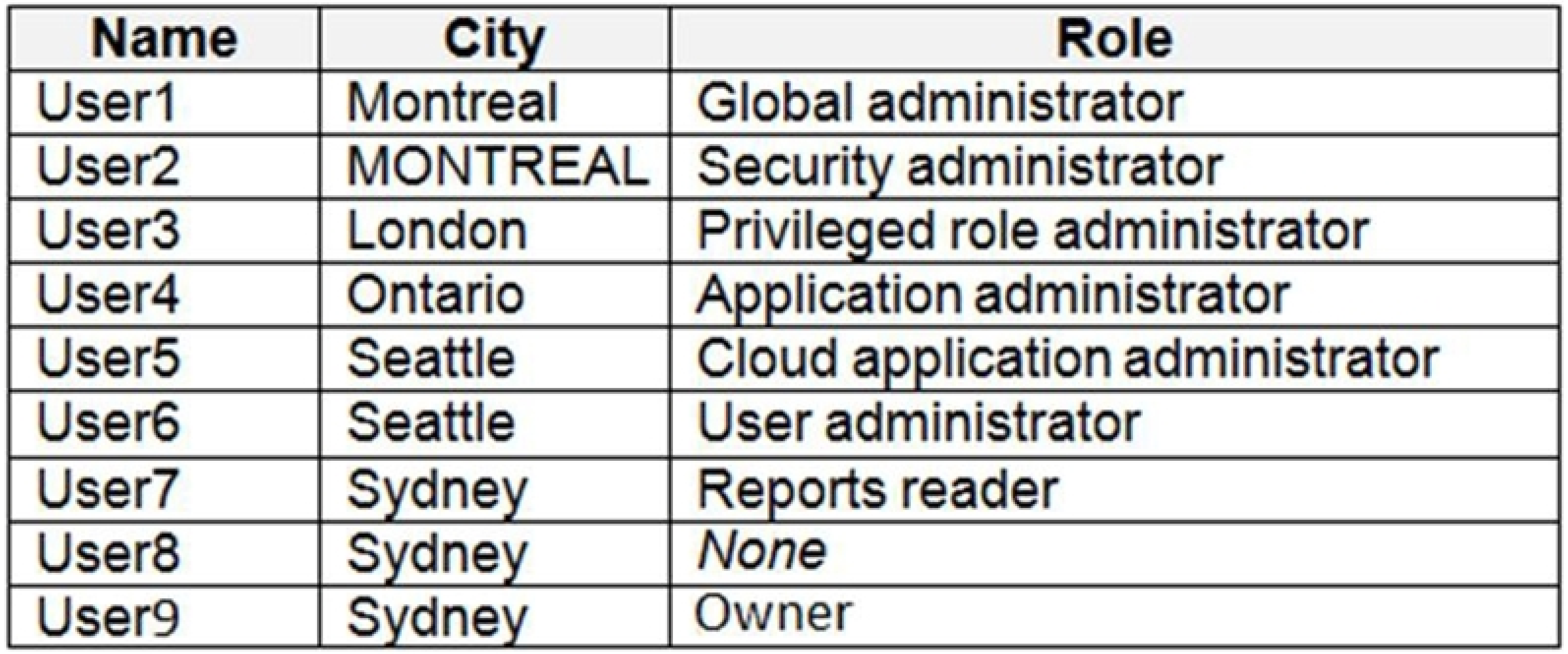
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/notebooks

QUESTION 2
From Azure Security Center, you need to deploy SecPol1.
What should you do first?

A. Enable Azure Defender.
B. Create an Azure Management group.
C. Create an initiative.
D. Configure continuous export.

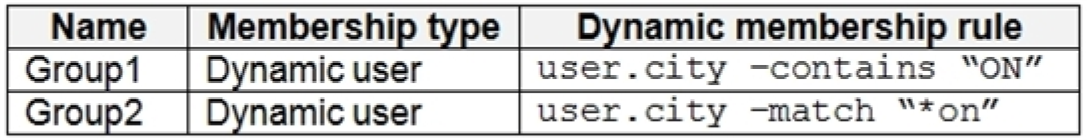
Correct Answer: C
Section:
Explanation:
Reference:
https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/security-center/custom-security-policies.md
https://zimmergren.net/create-custom-security-center-recommendation-with-azure-policy/

02 - Manage security operations
Case Study
This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.
To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.
At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.
To start the case study
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.
Overview
Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.
The company hosts its entire server infrastructure in Azure.
Contoso has two Azure subscriptions named Sub1 and Sub2. Both subscriptions are associated to an Azure Active Directory (Azure AD) tenant named contoso.com.
Existing Environment
Azure AD
Contoso.com contains the users shown in the following table.



Name	City	Role
User1	Montreal	Global administrator
User2	MONTREAL	Security administrator
User3	London	Privileged role administrator
User4	Ontario	Application administrator
User5	Seattle	Cloud application administrator
User6	Seattle	User administrator
User7	Sydney	Reports reader
User8	Sydney	*None*
User9	Sydney	Owner

Contoso.com contains the security groups shown in the following table.

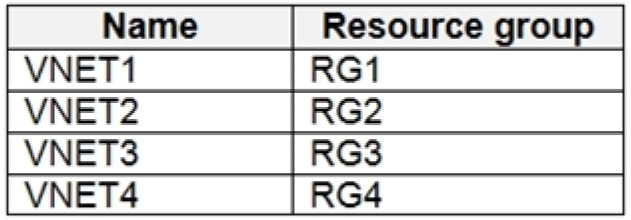


Name	Membership type	Dynamic membership rule
Group1	Dynamic user	`user.city -contains “ON”`
Group2	Dynamic user	`user.city -match “*on”`

Sub1

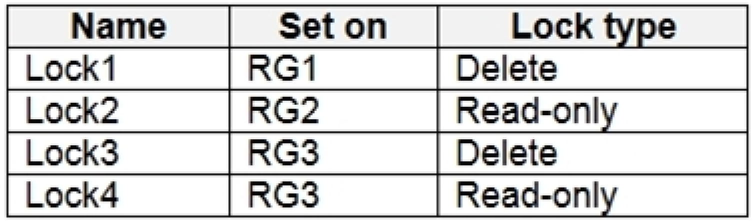
Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6.

User9 creates the virtual networks shown in the following table.



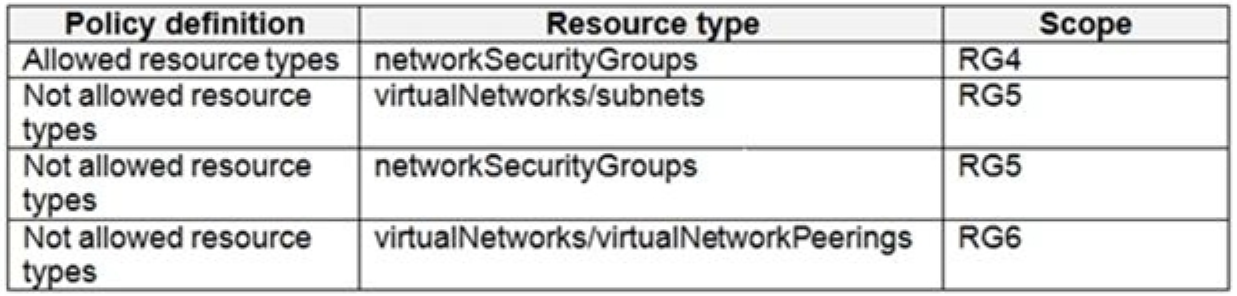
Name	Resource group
VNET1	RG1
VNET2	RG2
VNET3	RG3
VNET4	RG4

Sub1 contains the locks shown in the following table.



Name	Set on	Lock type
Lock1	RG1	Delete
Lock2	RG2	Read-only
Lock3	RG3	Delete
Lock4	RG3	Read-only

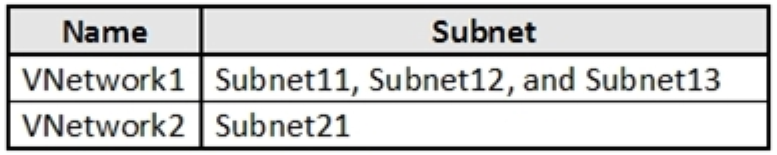
Sub1 contains the Azure policies shown in the following table.



Policy definition	Resource type	Scope
Allowed resource types	networkSecurityGroups	RG4
Not allowed resource types	virtualNetworks/subnets	RG5
Not allowed resource types	networkSecurityGroups	RG5
Not allowed resource types	virtualNetworks/virtualNetworkPeerings	RG6

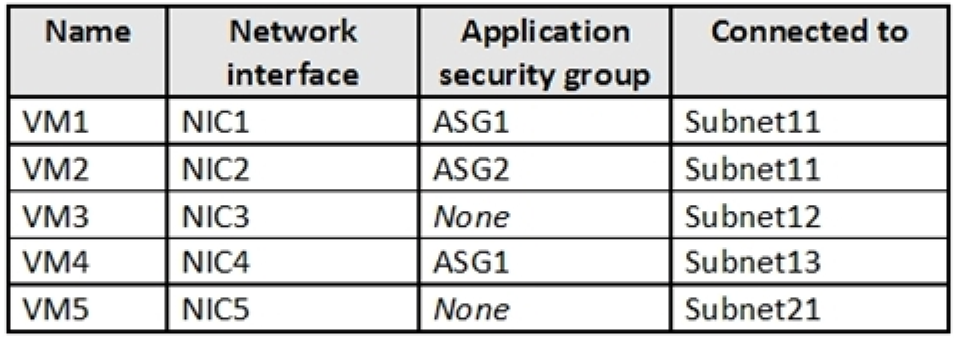
Sub2

Sub2 contains the virtual networks shown in the following table.



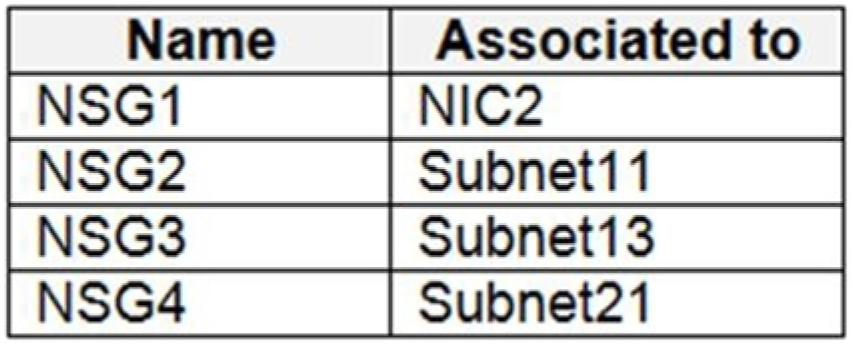
Name	Subnet
VNetwork1	Subnet11, Subnet12, and Subnet13
VNetwork2	Subnet21

Sub2 contains the virtual machines shown in the following table.



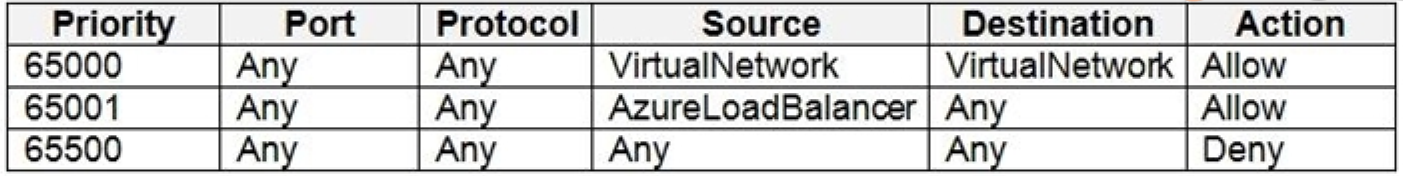
Name	Network interface	Application security group	Connected to
VM1	NIC1	ASG1	Subnet11
VM2	NIC2	ASG2	Subnet11
VM3	NIC3	*None*	Subnet12
VM4	NIC4	ASG1	Subnet13
VM5	NIC5	*None*	Subnet21

All virtual machines have public IP addresses and the Web Server (IIS) role installed. The firewalls for each virtual machine allow ping requests and web requests.
Sub2 contains the network security groups (NSGs) shown in the following table.



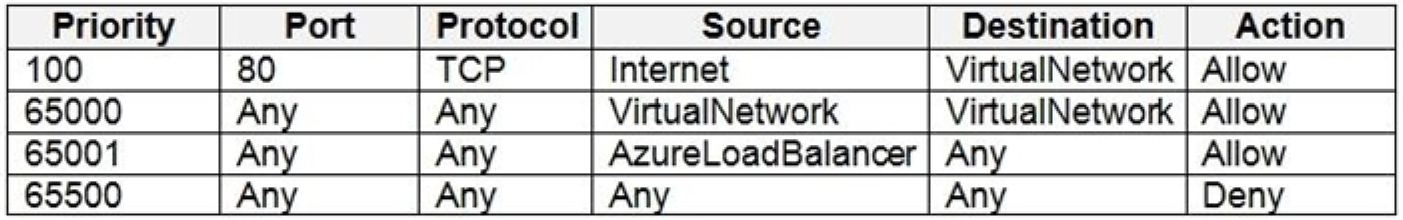
Name	Associated to
NSG1	NIC2
NSG2	Subnet11
NSG3	Subnet13
NSG4	Subnet21

NSG1 has the inbound security rules shown in the following table.



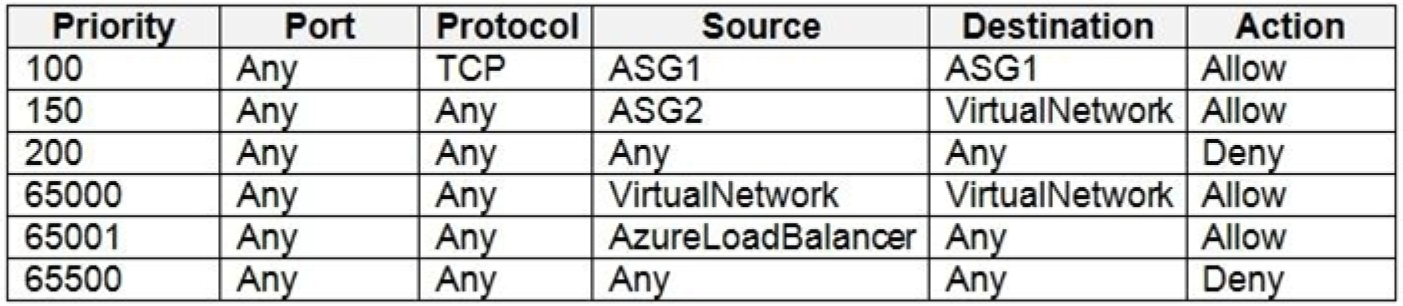
Priority	Port	Protocol	Source	Destination	Action
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG2 has the inbound security rules shown in the following table.



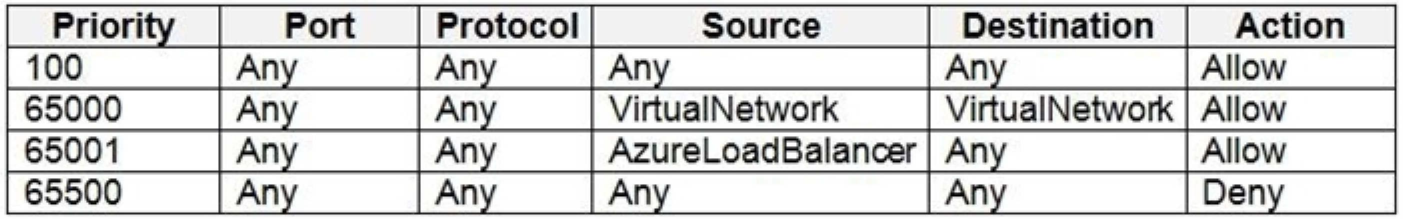
Priority	Port	Protocol	Source	Destination	Action
100	80	TCP	Internet	VirtualNetwork	Allow
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG3 has the inbound security rules shown in the following table.



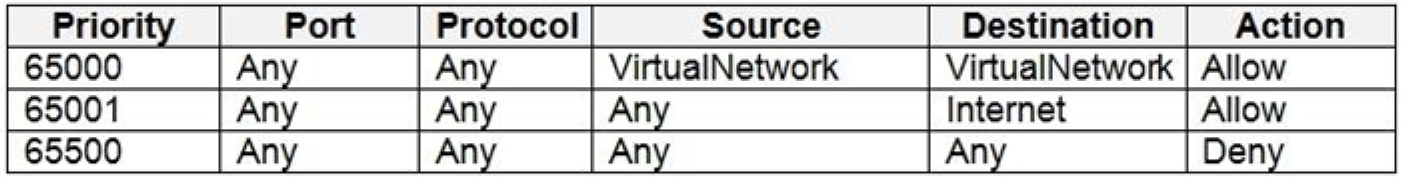
Priority	Port	Protocol	Source	Destination	Action
100	Any	TCP	ASG1	ASG1	Allow
150	Any	Any	ASG2	VirtualNetwork	Allow
200	Any	Any	Any	Any	Deny
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG4 has the inbound security rules shown in the following table.



Priority	Port	Protocol	Source	Destination	Action
100	Any	Any	Any	Any	Allow
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG1, NSG2, NSG3, and NSG4 have the outbound security rules shown in the following table.



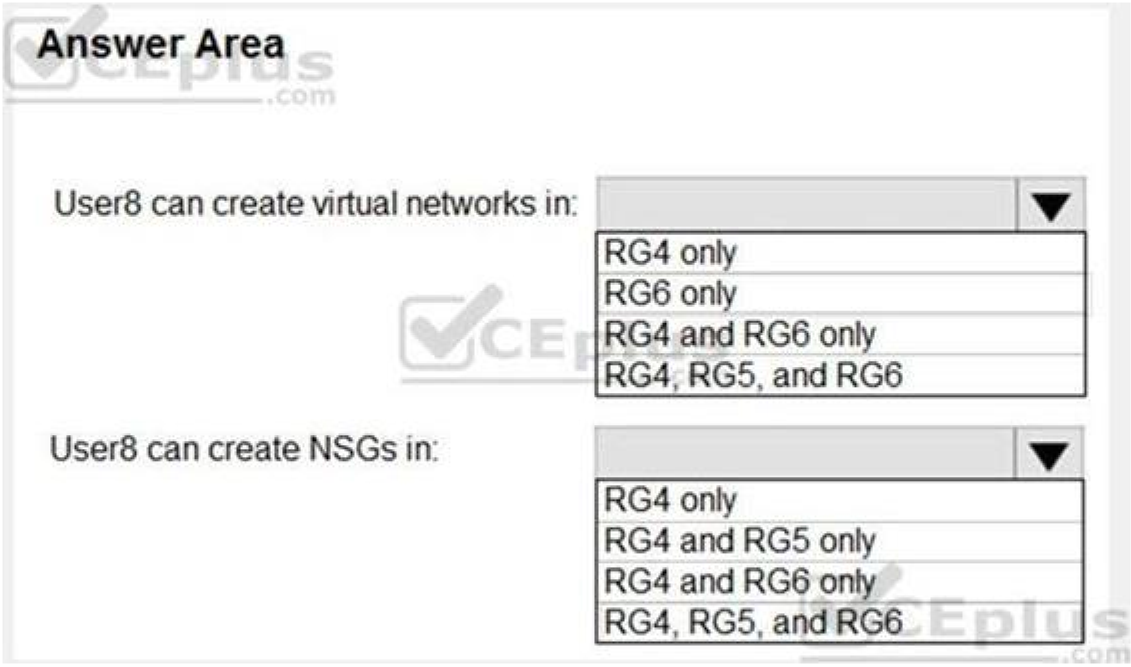
Priority	Port	Protocol	Source	Destination	Action
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	Any	Internet	Allow
65500	Any	Any	Any	Any	Deny

Technical requirements
Contoso identifies the following technical requirements:
Deploy Azure Firewall to VNetwork1 in Sub2.
Register an application named App2 in contoso.com.
Whenever possible, use the principle of least privilege.
Enable Azure AD Privileged Identity Management (PIM) for contoso.com.

QUESTION 1

You assign User8 the Owner role for RG4, RG5, and RG6.In which resource groups can User8 create virtual networks and NSGs? You must be able to connect virtual machines to deployed virtual networks. To answer, select the appropriate options in the answer area.NOTE: Each correct selection is worth one point.

Hot Area:

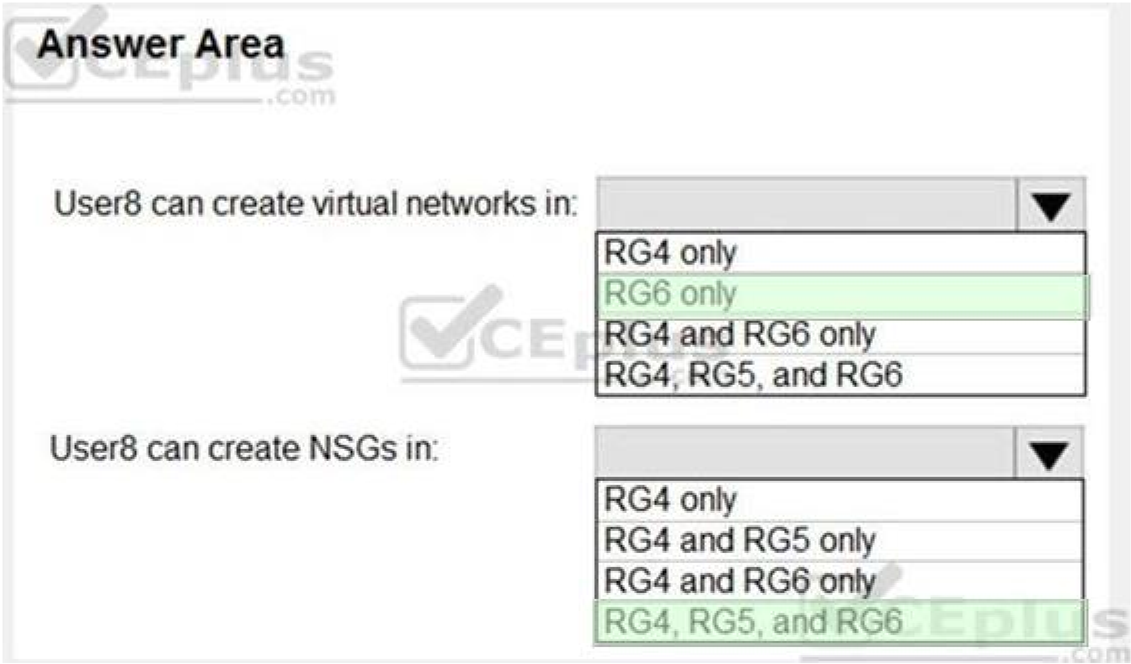


Answer Area

User8 can create virtual networks in:
- RG4 only
- RG6 only
- RG4 and RG6 only
- RG4, RG5, and RG6

User8 can create NSGs in:
- RG4 only
- RG4 and RG5 only
- RG4 and RG6 only
- RG4, RG5, and RG6

Answer Area:



Answer Area

User8 can create virtual networks in:

- RG4 only
- [✓ RG6 only]
- RG4 and RG6 only
- RG4, RG5, and RG6

User8 can create NSGs in:

- RG4 only
- RG4 and RG5 only
- RG4 and RG6 only
- [✓ RG4, RG5, and RG6]

Section:

Explanation:

Box 1: RG6 only

The policy does not allow the creation of virtual networks/subnets in RG5. Only NSGs can be created in RG4.B

Box 2: Rg4,Rg5, and Rg6

Scenario:

Contoso has two Azure subscriptions named Sub1 and Sub2.

Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6.

You assign User8 the Owner role for RG4, RG5, and RG6

User8 city Sidney, Role:None

Note: A network security group (NSG) contains a list of security rules that allow or deny network traffic to resources connected to Azure Virtual Networks (VNet). NSGs can be associated to subnets, individual VMs (classic), or individual network interfaces (NIC) attached to VMs (Resource Manager).

References:

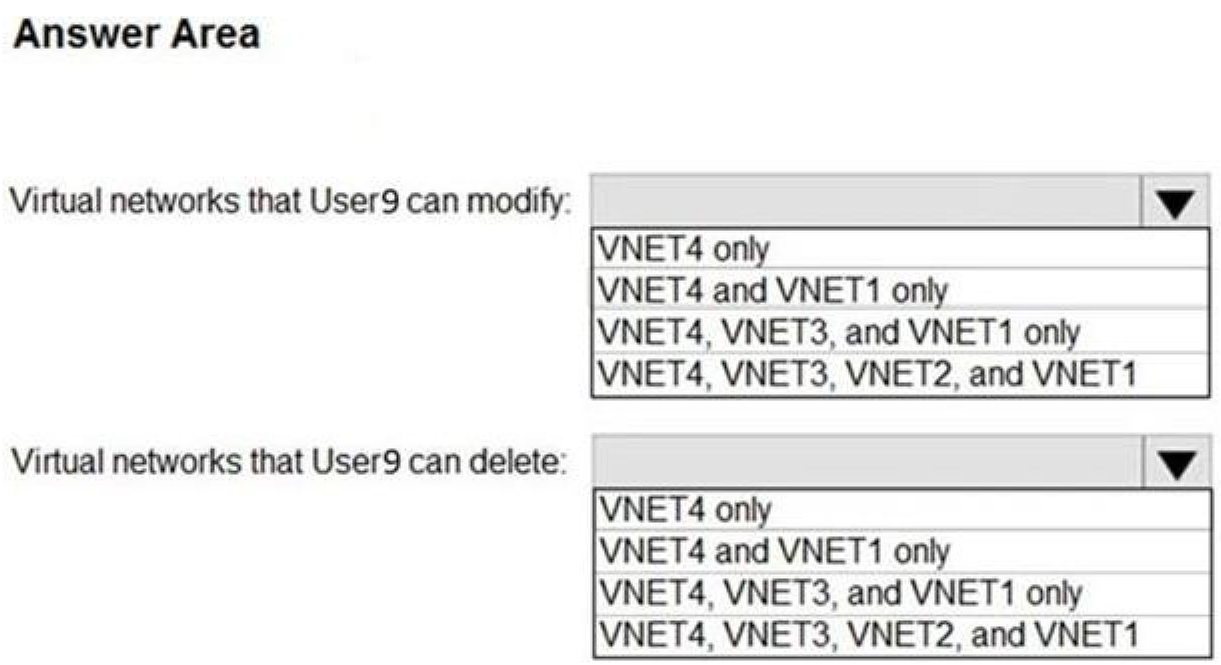
https://docs.microsoft.com/en-us/azure/governance/policy/overview

QUESTION 2

Which virtual networks in Sub1 can User9 modify and delete in their current state? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

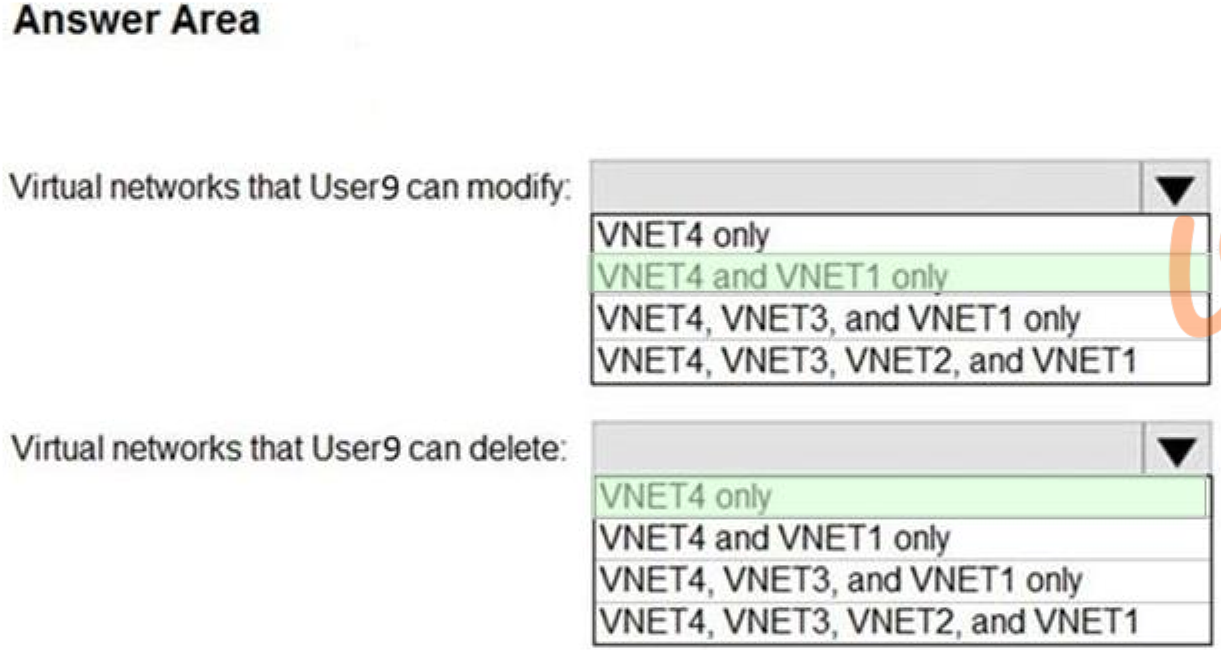
Virtual networks that User9 can modify: ▼

VNET4 only
VNET4 and VNET1 only
VNET4, VNET3, and VNET1 only
VNET4, VNET3, VNET2, and VNET1

Virtual networks that User9 can delete: ▼

VNET4 only
VNET4 and VNET1 only
VNET4, VNET3, and VNET1 only
VNET4, VNET3, VNET2, and VNET1

Answer Area:



Answer Area

Virtual networks that User9 can modify: ▼

VNET4 only
[✓ VNET4 and VNET1 only]
VNET4, VNET3, and VNET1 only
VNET4, VNET3, VNET2, and VNET1

Virtual networks that User9 can delete: ▼

[✓ VNET4 only]
VNET4 and VNET1 only
VNET4, VNET3, and VNET1 only
VNET4, VNET3, VNET2, and VNET1

Section:

Explanation:

Box 1: VNET4 and VNET1 only

RG1 has only Delete lock, while there are no locks on RG4.

RG2 and RG3 both have Read-only locks.

Box 2: VNET4 only

There are no locks on RG4, while the other resource groups have either Delete or Read-only locks.

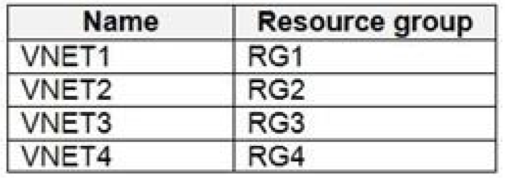
Note: As an administrator, you may need to lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources. You can set the lock level to CanNotDelete or ReadOnly. In the portal, the locks are called Delete and Read-only respectively.

CanNotDelete means authorized users can still read and modify a resource, but they can't delete the resource. ReadOnly means authorized users can read a resource, but they can't delete or update the resource. Applying this lock is similar to restricting all authorized users to the permissions granted by the Reader role.

Scenario:

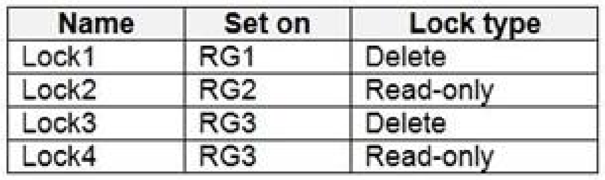
Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6.

User9 creates the virtual networks shown in the following table.



Name	Resource group
VNET1	RG1
VNET2	RG2
VNET3	RG3
VNET4	RG4

Sub1 contains the locks shown in the following table.



Name	Set on	Lock type
Lock1	RG1	Delete
Lock2	RG2	Read-only
Lock3	RG3	Delete
Lock4	RG3	Read-only

Reference:

https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources

03 - Manage security operations

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

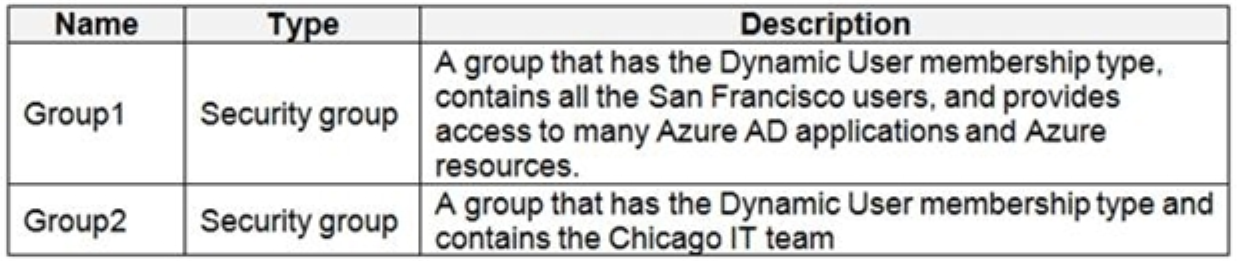
Litware, Inc. is a digital media company that has 500 employees in the Chicago area and 20 employees in the San Francisco area.

Existing Environment

Litware has an Azure subscription named Sub1 that has a subscription ID of 43894a43-17c2-4a39-8cfc-3540c2653ef4.

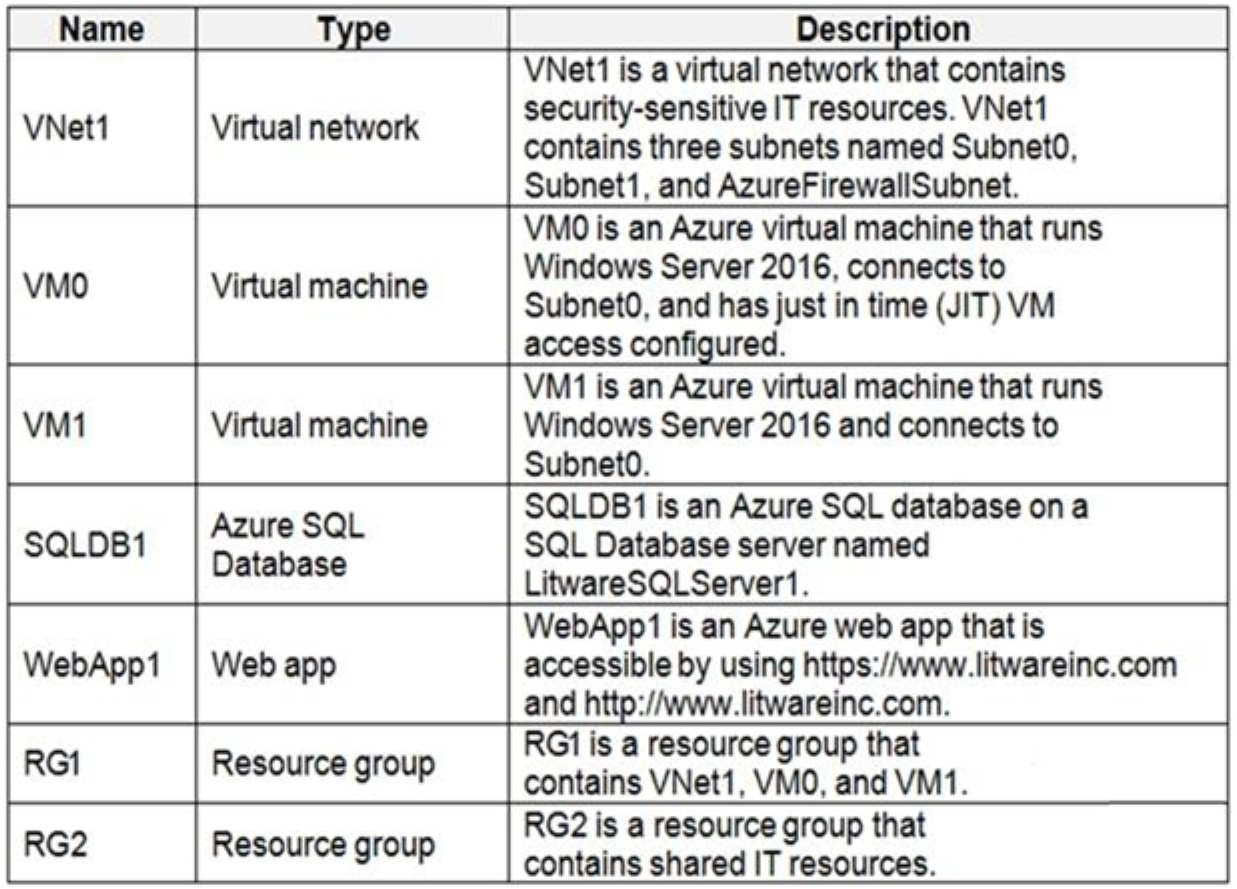
Sub1 is associated to an Azure Active Directory (Azure AD) tenant named litwareinc.com. The tenant contains the user objects and the device objects of all the Litware employees and their devices. Each user is assigned an Azure AD Premium P2 license. Azure AD Privileged Identity Management (PIM) is activated.

The tenant contains the groups shown in the following table.



Name	Type	Description
Group1	Security group	A group that has the Dynamic User membership type, contains all the San Francisco users, and provides access to many Azure AD applications and Azure resources.
Group2	Security group	A group that has the Dynamic User membership type and contains the Chicago IT team

The Azure subscription contains the objects shown in the following table.



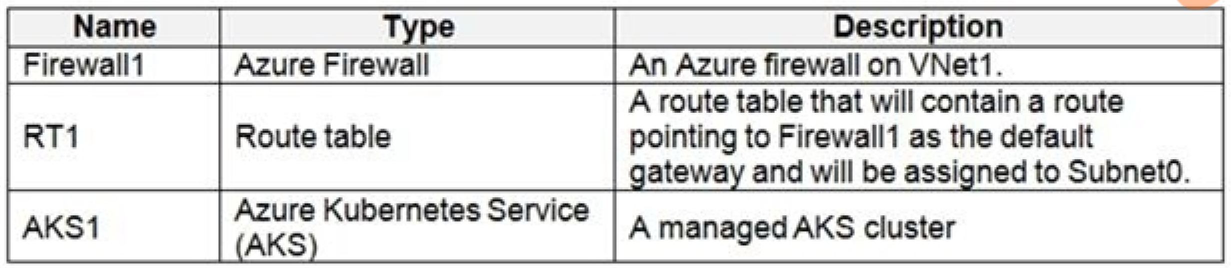
Name	Type	Description
VNet1	Virtual network	VNet1 is a virtual network that contains security-sensitive IT resources. VNet1 contains three subnets named Subnet0, Subnet1, and AzureFirewallSubnet.
VM0	Virtual machine	VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured.
VM1	Virtual machine	VM1 is an Azure virtual machine that runs Windows Server 2016 and connects to Subnet0.
SQLDB1	Azure SQL Database	SQLDB1 is an Azure SQL database on a SQL Database server named LitwareSQLServer1.
WebApp1	Web app	WebApp1 is an Azure web app that is accessible by using https://www.litwareinc.com and http://www.litwareinc.com.
RG1	Resource group	RG1 is a resource group that contains VNet1, VM0, and VM1.
RG2	Resource group	RG2 is a resource group that contains shared IT resources.

Azure Security Center is set to the Standard tier.

Requirements

Planned Changes

Litware plans to deploy the Azure resources shown in the following table.



Name	Type	Description
Firewall1	Azure Firewall	An Azure firewall on VNet1.
RT1	Route table	A route table that will contain a route pointing to Firewall1 as the default gateway and will be assigned to Subnet0.
AKS1	Azure Kubernetes Service (AKS)	A managed AKS cluster

Identity and Access Requirements

Litware identifies the following identity and access requirements:

All San Francisco users and their devices must be members of Group1.

The members of Group2 must be assigned the Contributor role to RG2 by using a permanent eligible assignment. Users must be prevented from registering applications in Azure AD and from consenting to applications that access company information on the users' behalf.

Platform Protection Requirements

Litware identifies the following platform protection requirements:

Microsoft Antimalware must be installed on the virtual machines in RG1.

The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role.

Azure AD users must be able to authenticate to AKS1 by using their Azure AD credentials.

Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access. A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in RG1. Role1 must be available only for RG1.

Security Operations Requirements

Litware must be able to customize the operating system security configurations in Azure Security Center. Data and Application Requirements

Litware identifies the following data and applications requirements:

The users in Group2 must be able to authenticate to SQLDB1 by using their Azure AD credentials.

WebApp1 must enforce mutual authentication.

General Requirements

Litware identifies the following general requirements:
Whenever possible, administrative effort must be minimized.
Whenever possible, use of automation must be maximized.

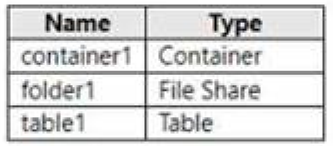
QUESTION 1
You need to ensure that you can meet the security operations requirements. What should you do first?

A. Turn on Auto Provisioning in Security Center.
B. Integrate Security Center and Microsoft Cloud App Security.
C. Upgrade the pricing tier of Security Center to Standard.
D. Modify the Security Center workspace configuration.

Correct Answer: C
Section:
Explanation:
The Standard tier extends the capabilities of the Free tier to workloads running in private and other public clouds, providing unified security management and threat protection across your hybrid cloud workloads. The Standard tier also adds advanced threat detection capabilities, which uses built-in behavioral analytics and machine learning to identify attacks and zero-days exploits, access and application controls to reduce exposure to network attacks and malware, and more.
Scenario: Security Operations Requirements
Litware must be able to customize the operating system security configurations in Azure Security Center.
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-pricing

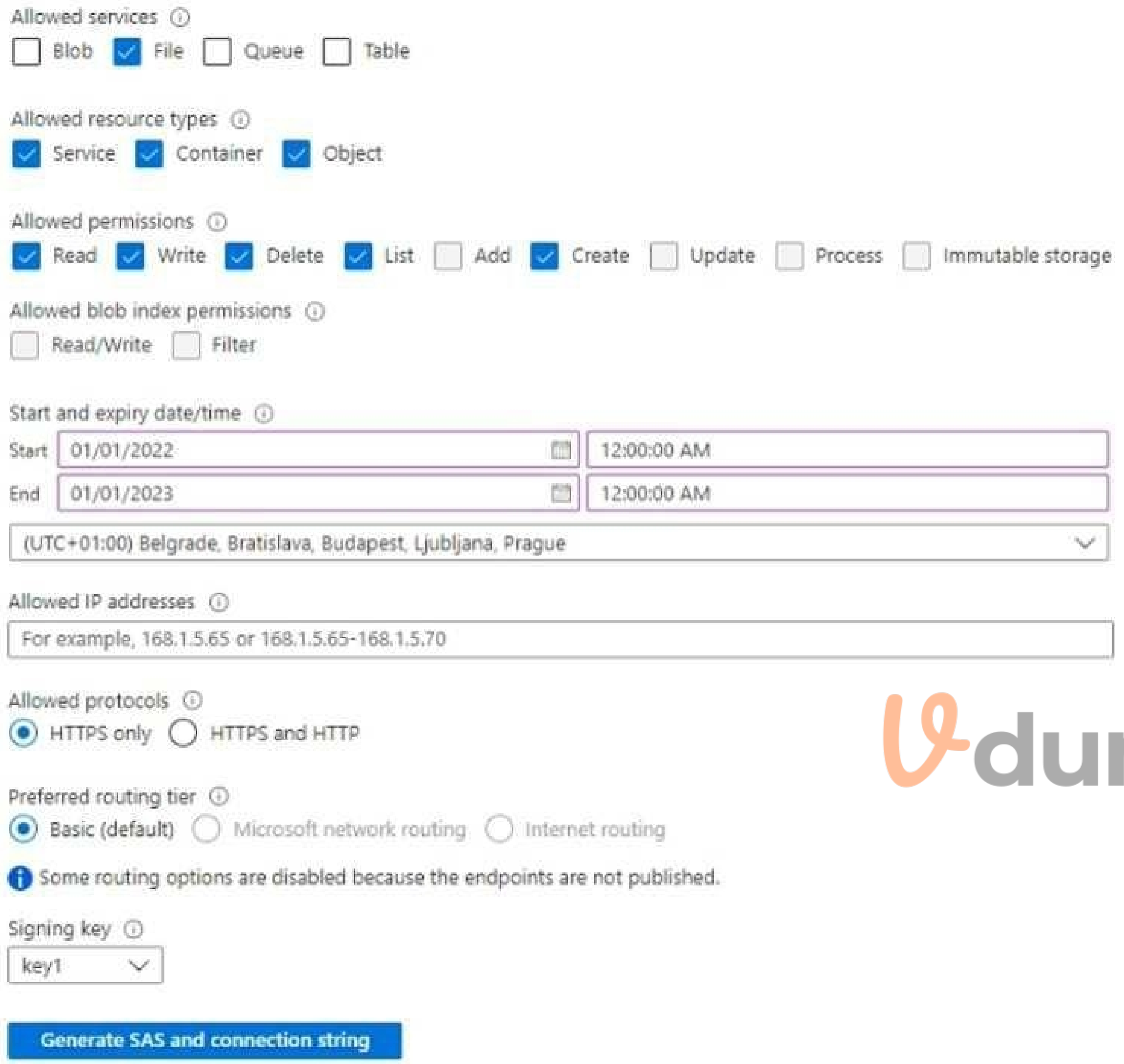
Exam K

QUESTION 1
HOTSPOT
You have an Azure subscription that contains a user named User1 and a storage account named storage1. The storage1 account contains the resources shown in the following table.



Name	Type
container1	Container
folder1	File Share
table1	Table

In storage1, you create a shared access signature (SAS) named SAS1 as shown in the following exhibit.



Allowed services ⓘ

□ Blob ☑ File □ Queue □ Table

Allowed resource types ⓘ

☑ Service ☑ Container ☑ Object

Allowed permissions ⓘ

☑ Read ☑ Write ☑ Delete ☑ List □ Add ☑ Create □ Update □ Process □ Immutable storage

Allowed blob index permissions ⓘ

□ Read/Write □ Filter

Start and expiry date/time ⓘ

Start 01/01/2022 12:00:00 AM

End 01/01/2023 12:00:00 AM

(UTC+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague

Allowed IP addresses ⓘ

For example, 168.1.5.65 or 168.1.5.65-168.1.5.70

Allowed protocols ⓘ

● HTTPS only ○ HTTPS and HTTP

Preferred routing tier ⓘ

● Basic (default) ○ Microsoft network routing ○ Internet routing

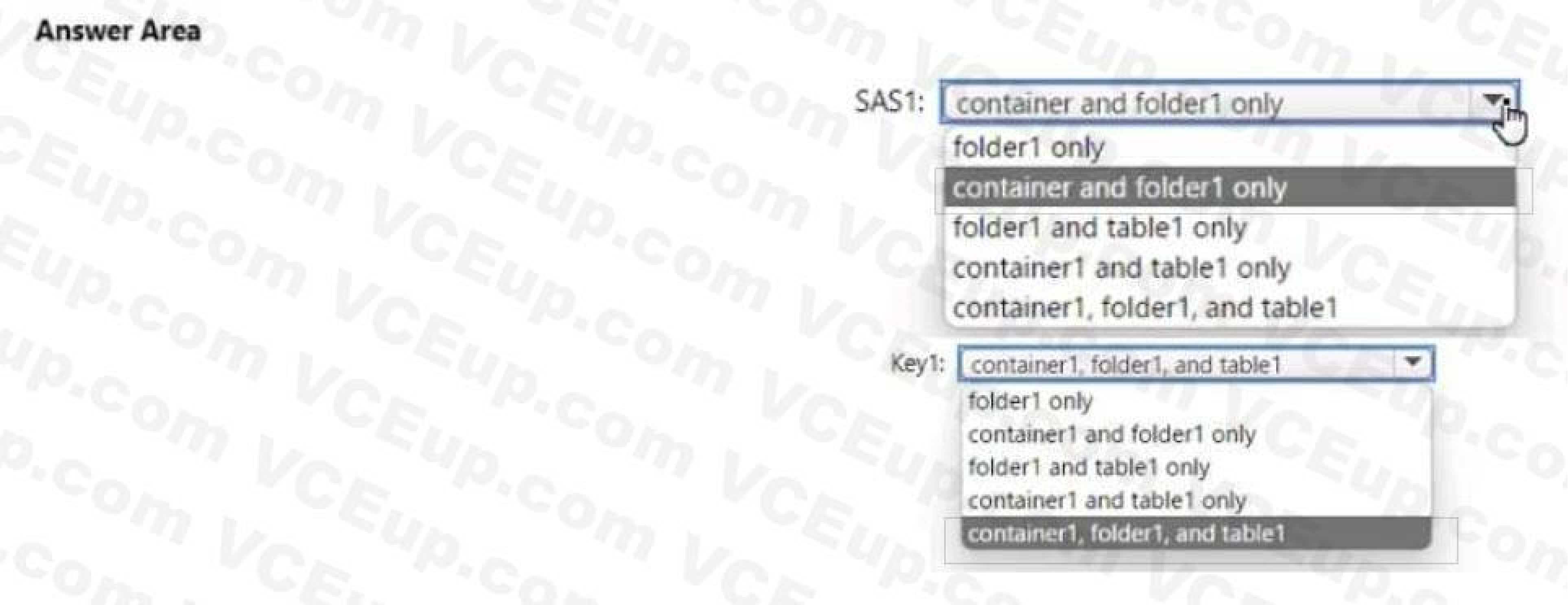
ⓘ Some routing options are disabled because the endpoints are not published.

Signing key ⓘ

key1

To which resources can User! write on July 1, 2022 by using SAS1 and key 1? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

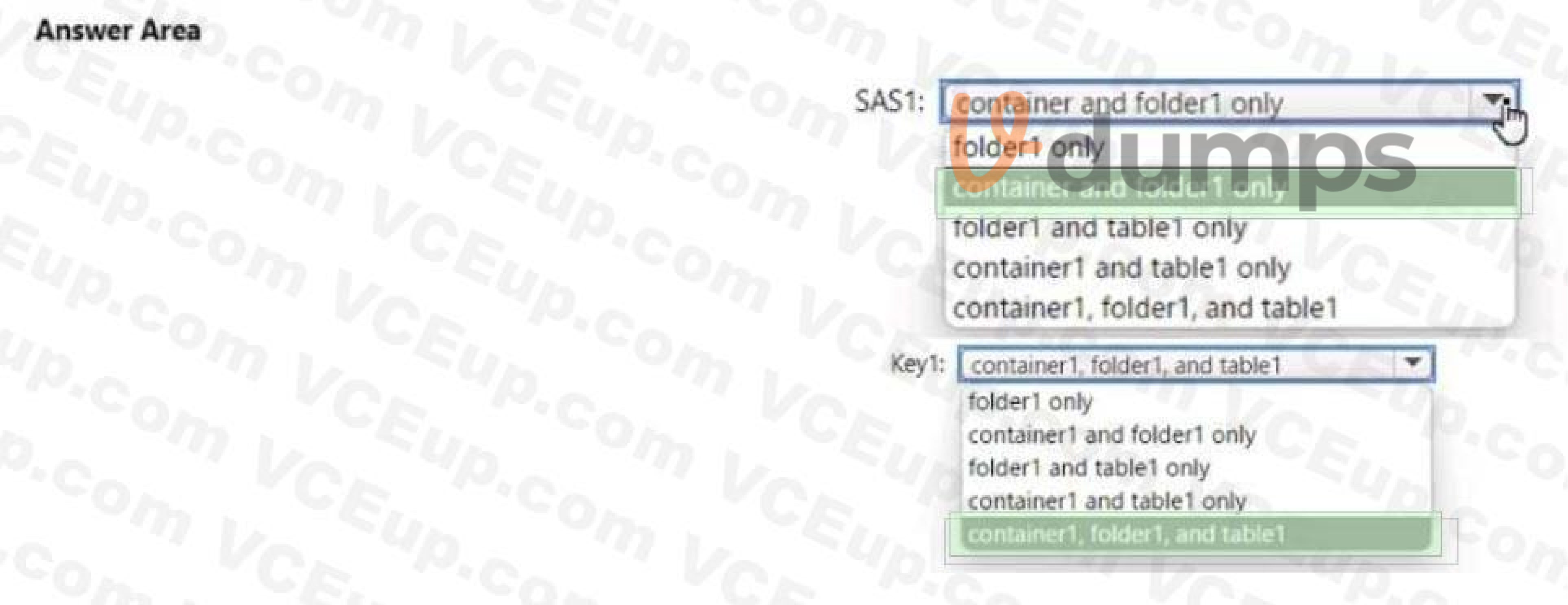
SAS1: container and folder1 only

- folder1 only
- container and folder1 only
- folder1 and table1 only
- container1 and table1 only
- container1, folder1, and table1

Key1: container1, folder1, and table1

- folder1 only
- container1 and folder1 only
- folder1 and table1 only
- container1 and table1 only
- container1, folder1, and table1

Answer Area:



Answer Area

SAS1: container and folder1 only

- folder1 only
- container and folder1 only
- folder1 and table1 only
- container1 and table1 only
- container1, folder1, and table1

Key1: container1, folder1, and table1

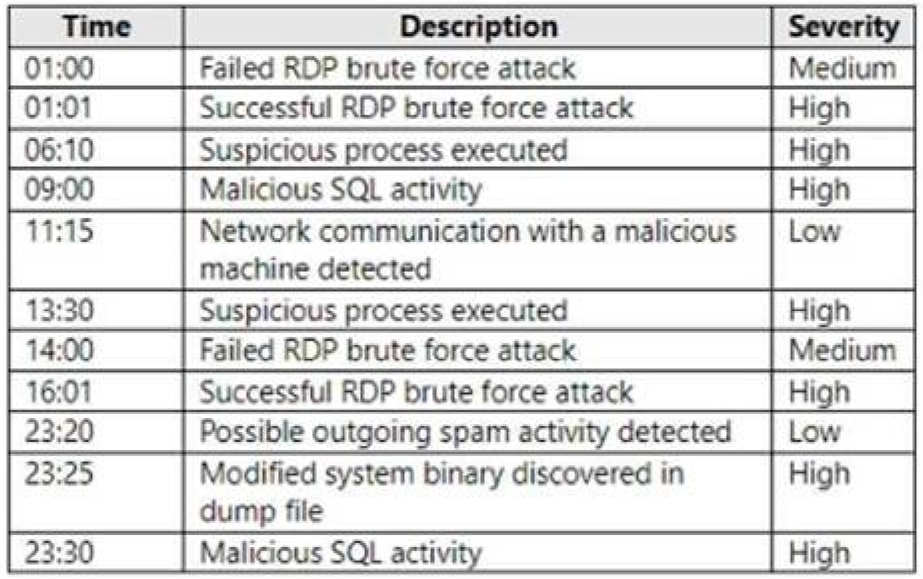
- folder1 only
- container1 and folder1 only
- folder1 and table1 only
- container1 and table1 only
- container1, folder1, and table1

Section:
Explanation:

QUESTION 2

HOTSPOT

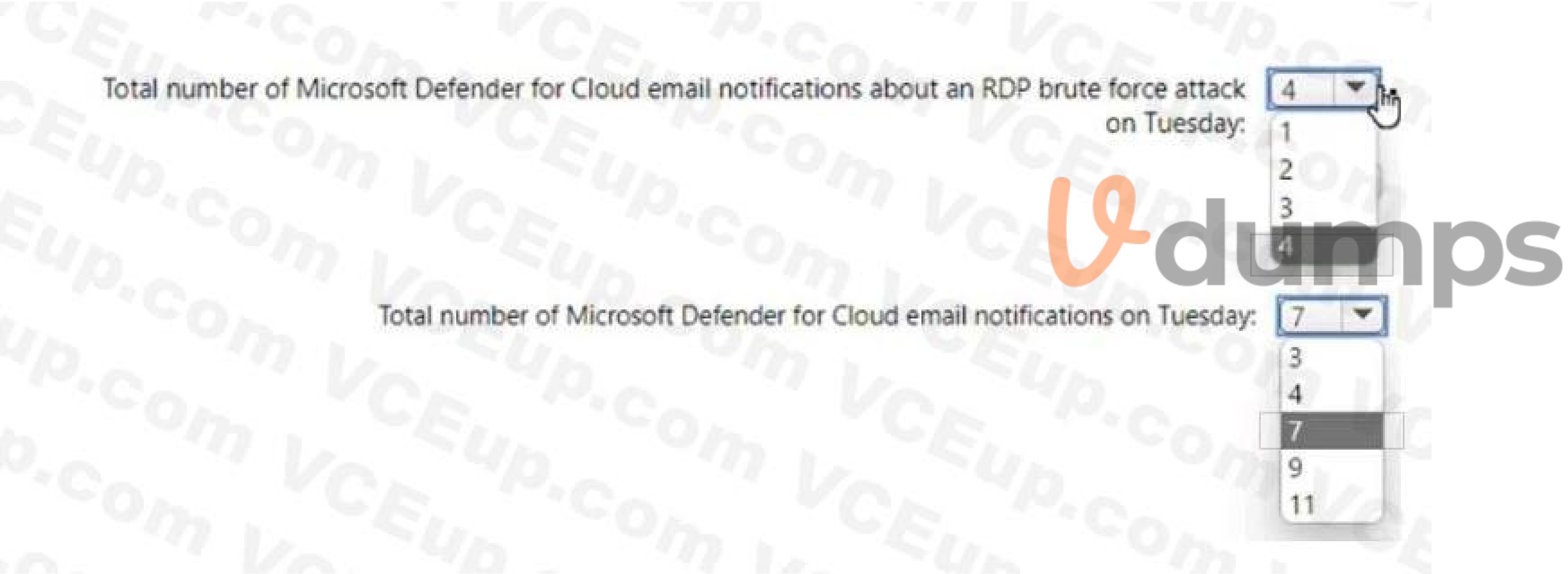
On Monday, you configure an email notification in Microsoft Defender for Cloud to notify user1 @contoso.com about alerts that have a severity level of Low, Medium, or High. On Tuesday, Microsoft Defender for Cloud generates the security alerts shown in the following table.



Time	Description	Severity
01:00	Failed RDP brute force attack	Medium
01:01	Successful RDP brute force attack	High
06:10	Suspicious process executed	High
09:00	Malicious SQL activity	High
11:15	Network communication with a malicious machine detected	Low
13:30	Suspicious process executed	High
14:00	Failed RDP brute force attack	Medium
16:01	Successful RDP brute force attack	High
23:20	Possible outgoing spam activity detected	Low
23:25	Modified system binary discovered in dump file	High
23:30	Malicious SQL activity	High

How many email notifications will user1 @contoso.com receive on Tuesday? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

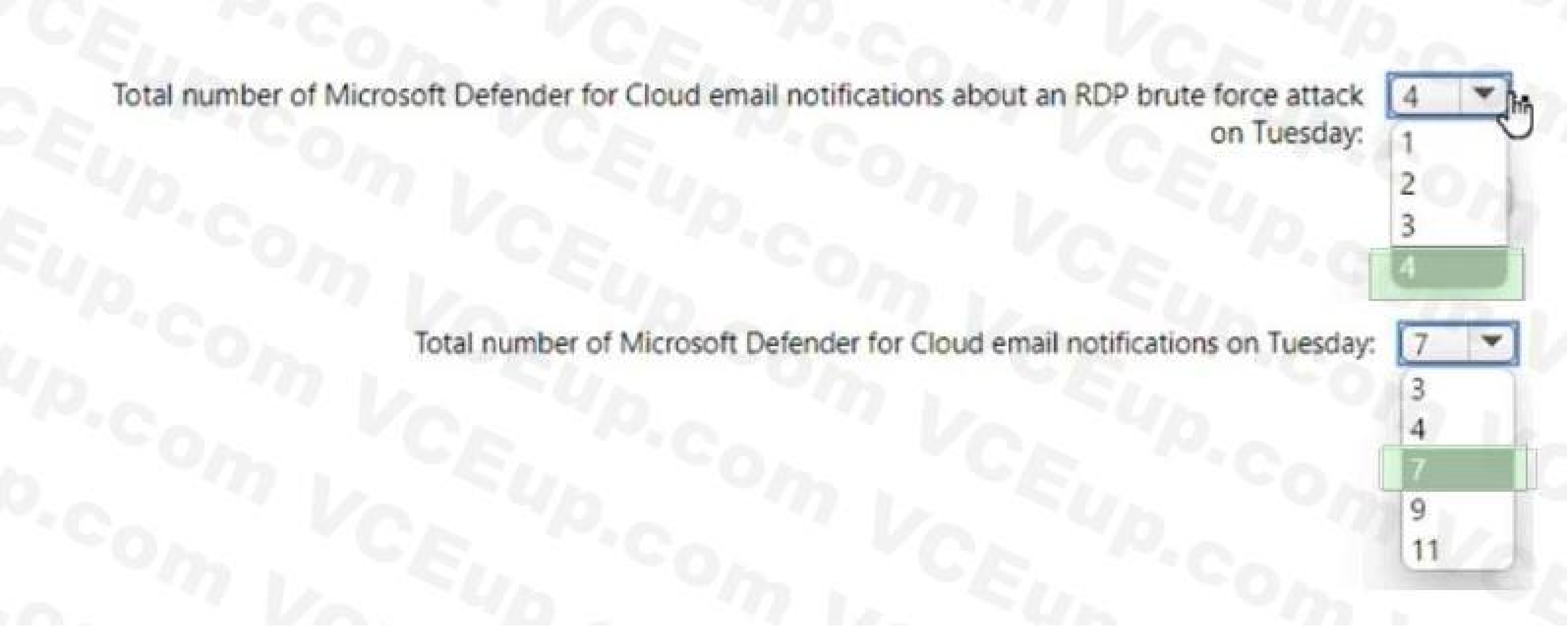
Hot Area:



Total number of Microsoft Defender for Cloud email notifications about an RDP brute force attack on Tuesday: 4

Total number of Microsoft Defender for Cloud email notifications on Tuesday: 7

Answer Area:

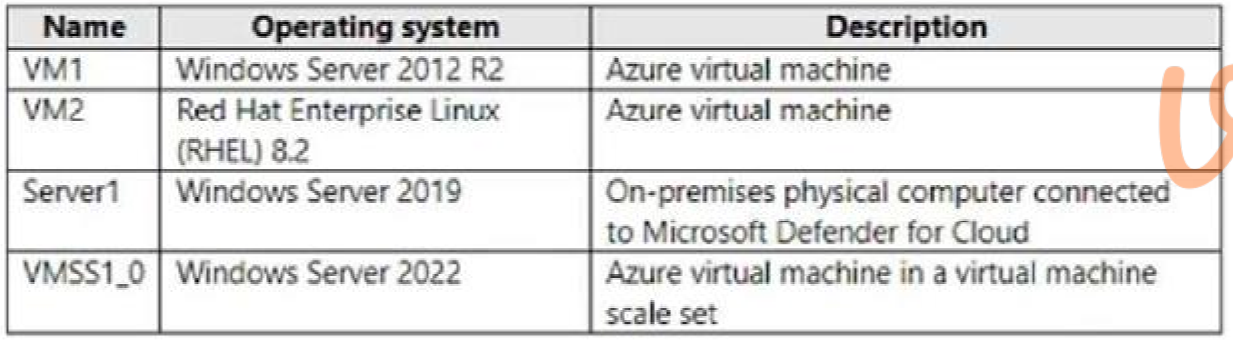


Total number of Microsoft Defender for Cloud email notifications about an RDP brute force attack on Tuesday: 4

Total number of Microsoft Defender for Cloud email notifications on Tuesday: 7

Section:
Explanation:

QUESTION 3
You have an Azure subscription and the computers shown in the following table.



Name	Operating system	Description
VM1	Windows Server 2012 R2	Azure virtual machine
VM2	Red Hat Enterprise Linux (RHEL) 8.2	Azure virtual machine
Server1	Windows Server 2019	On-premises physical computer connected to Microsoft Defender for Cloud
VMSS1_0	Windows Server 2022	Azure virtual machine in a virtual machine scale set

You need to perform a vulnerability scan of the computers by using Microsoft Defender for Cloud.
Which computers can you scan?

A. VM1 only
B. VM1 and VM2 only
C. Server1 and VMSS1.0 only
D. VM1, VM2, and Server1 only
E. VM1, VM2, Server1, and VMSS1.0

Correct Answer: A
Section:

QUESTION 4
You have an Azure subscription that contains an Azure web app named 1 and a virtual machine named VM1. VM1 runs Microsoft SQL Server and is connected to a virtual network named VNet1.
App1, VM1, and Vent are in the US Central Azure region.
You need to ensure that App1 can connect to VM1. The solution must minimize costs.

A. NAT gateway integration

B. Azure Front Door
C. regional virtual network integration
D. gateway-required virtual network integration
E. Azure Application Gateway integration

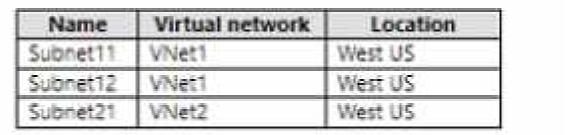
Correct Answer: C
Section:

QUESTION 5
You have an Azure subscription that contains a storage account and an Azure web app named App1.
App1 connects to an Azure Cosmos DB database named Cosmos1 that uses a private endpoint named Endpoint1. Endpoint1 has the default settings.
You need to validate the name resolution to Cosmos1.
Which DNS zone should you use?

A. Endpoint1. Privatelink,blob,core,windows,net
B. Endpoint1. Privatelink,database,azure,com
C. Endpoint1. Privatelink,azurewebsites,net
D. Endpoint1. Privatelink,documents,azure,com

Correct Answer: D
Section:

QUESTION 6
You have an Azure subscription that contains the subnets shown in the following table.



Name	Virtual network	Location
Subnet11	VNet1	West US
Subnet12	VNet1	West US
Subnet21	VNet2	West US

The subscription contains Azure web app named WebApp1 that has the following configurations.
* Region West Us
* Virtual network VNet1
* VNet integration on: Enabled
* Outbound subnet: Subnet11
* Windows plan (West US): ASP1
You plan to deploy an Azure web app named WebApp2 that will have the following settings:
* Region: West US
* VNet integration on-Enabled
* Windows plan (West UAS): WebApp2?
To which subnets can you integrate WebApp2?

A. Subnet11 only
B. Subnet2 only
C. Subnet11 or subnet12 only
D. Subnet2 or Subnet21 only
E. Subnet11, subnet2, or Subnet21

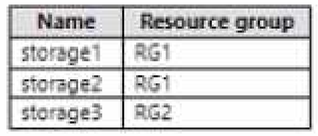
Correct Answer: C
Section:

QUESTION 7
You have an Azure AD turned that contains a user named User1.
You purchase an App named App1.
User1 needs to publish App1 by using Azure AD Application Proxy.
Which role should you assign to User1?

A. Hybrid identity Administrator
B. Cloud App Security Administrator
C. Application Administrator
D. Cloud Application Administrate

Correct Answer: C
Section:

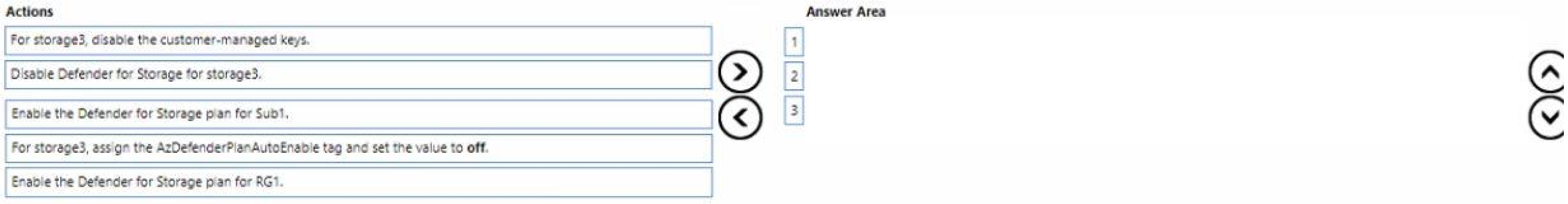
QUESTION 8
DRAG DROP
You have an Azure subscription named Sub1 that contains the storage accounts shown in the following table



Name	Resource group
storage1	RG1
storage2	RG1
storage3	RG2

The storage3 storage account is encrypted by using customer-managed keys.
YOU need to enable Microsoft Defender for storage to meet the following requirements.
* The storage1 and storage2 account must be include in the defender for storage requirement.
* The storage3 account must be exclude from the Defender for Storage protections.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and them in the correct order.

Select and Place:



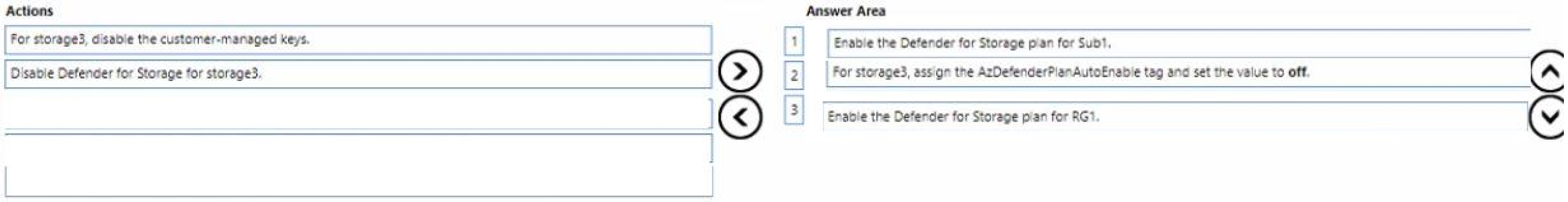
Actions

- For storage3, disable the customer-managed keys.
- Disable Defender for Storage for storage3.
- Enable the Defender for Storage plan for Sub1.
- For storage3, assign the AzDefenderPlanAutoEnable tag and set the value to **off**.
- Enable the Defender for Storage plan for RG1.

Answer Area

1
2
3

Correct Answer:



Actions

- For storage3, disable the customer-managed keys.
- Disable Defender for Storage for storage3.

Answer Area

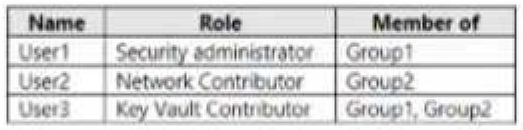
1 Enable the Defender for Storage plan for Sub1.
2 For storage3, assign the AzDefenderPlanAutoEnable tag and set the value to **off**.
3 Enable the Defender for Storage plan for RG1.

Section:
Explanation:

QUESTION 9

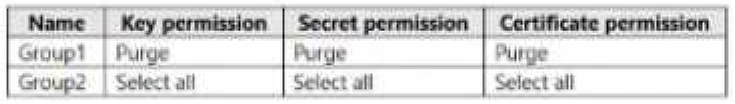
HOTSPOT

You have an Azure Subscription that is linked to an Azure Active Directory (Azure AD). The tenant contains the users shown in the following table.



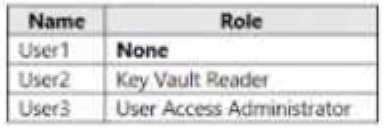
Name	Role	Member of
User1	Security administrator	Group1
User2	Network Contributor	Group2
User3	Key Vault Contributor	Group1, Group2

You have an Azure key vault named Vault1 that has Purge protection set to Disabled. Vault1 contains the access policies shown in the following table.



Name	Key permission	Secret permission	Certificate permission
Group1	Purge	Purge	Purge
Group2	Select all	Select all	Select all

You create role assignments for Vault1 as shown in the following table.

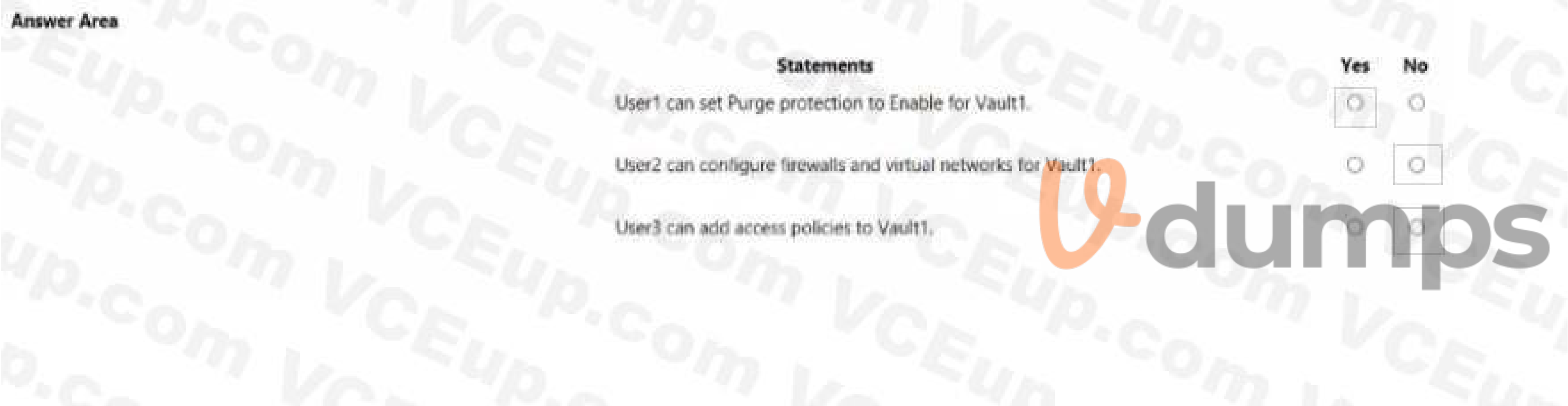


Name	Role
User1	**None**
User2	Key Vault Reader
User3	User Access Administrator

For each of the following statements, Yes if the statement is true, Otherwise, select No.

NOTE: Each correct selection is worth one point.

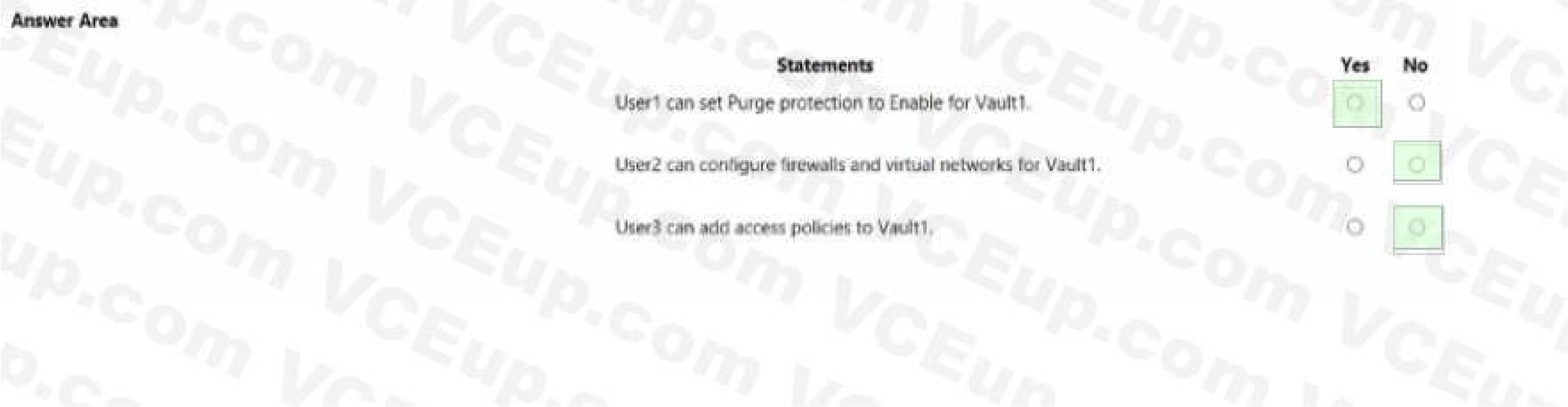
Hot Area:



Answer Area

Statements	Yes	No
User1 can set Purge protection to Enable for Vault1.	○	○
User2 can configure firewalls and virtual networks for Vault1.	○	○
User3 can add access policies to Vault1.	○	○

Answer Area:



Answer Area

Statements	Yes	No
User1 can set Purge protection to Enable for Vault1.	●	○
User2 can configure firewalls and virtual networks for Vault1.	○	●
User3 can add access policies to Vault1.	○	●

Section:

Explanation:

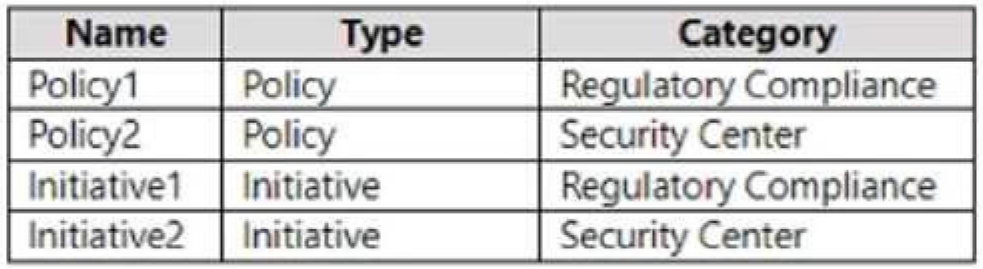
QUESTION 10

You have an Azure subscription that contains a Microsoft Defender External Attack Surface Management (Defender EASM) resource named EASM1. EASM1 has discovery enabled and contains several inventory assets. You need to identify which inventory assets are vulnerable to the most critical web app security risks. Which Defender EASM dashboard should you use?

A. Attack Surface Summary
B. GDPRCompliance
C. Security Posture
D. OWASPToplO

Correct Answer: D
Section:

QUESTION 11
You have an Azure subscription that uses Microsoft Defender for Cloud. The subscription contains the Azure Policy definitions shown in the following table.



Name	Type	Category
Policy1	Policy	Regulatory Compliance
Policy2	Policy	Security Center
Initiative1	Initiative	Regulatory Compliance
Initiative2	Initiative	Security Center

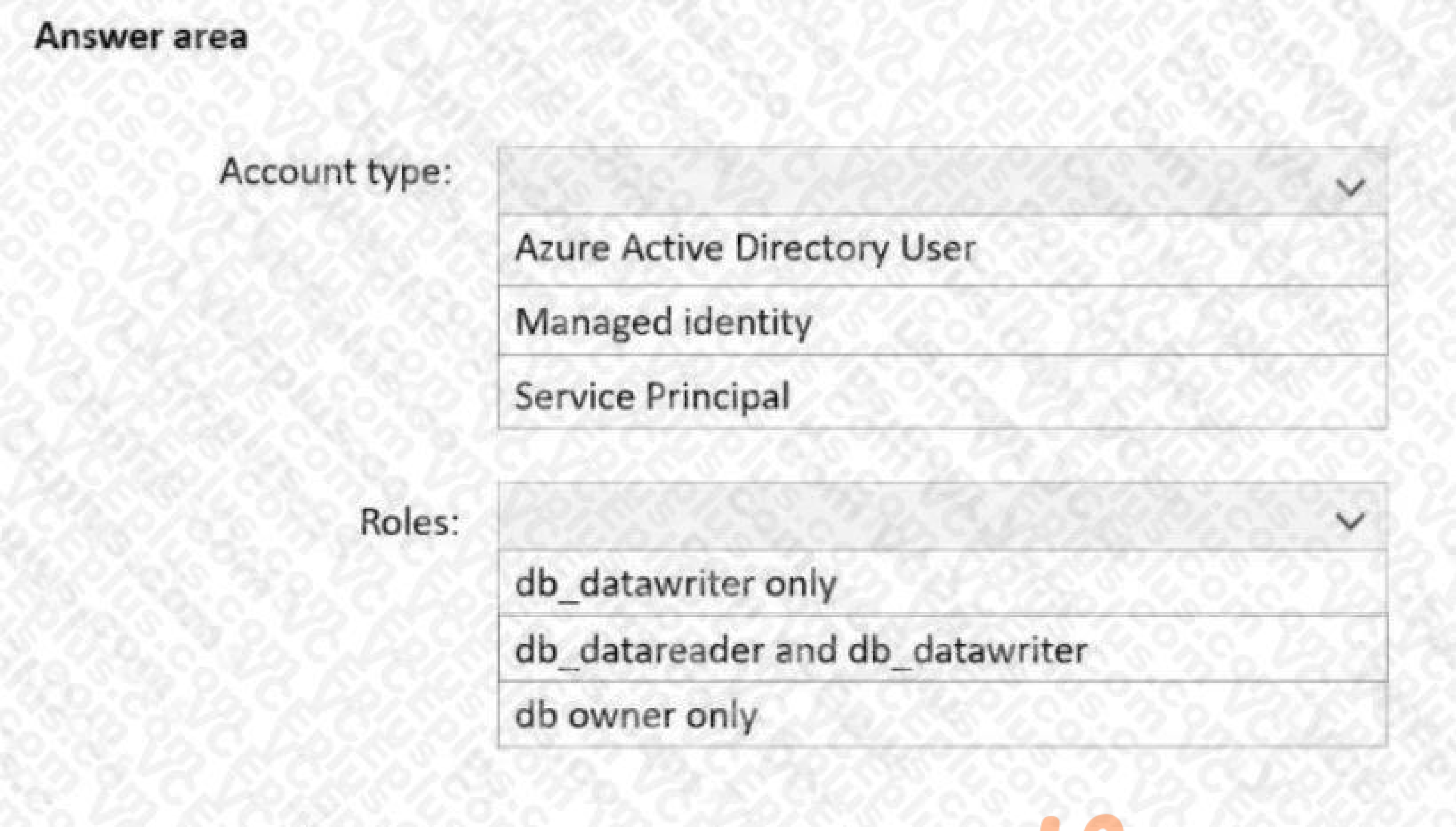
Which definitions can be assigned as a security policy in Defender for Cloud?

A. Policy1 and Policy2 only
B. Initiative1 and Initiative2 only
C. Policy1 and Initiative1 only
D. Policy2 and Initiative2 only
E. Policy1, Policy2, Initiative1, and Initiative2

Correct Answer: D
Section:

QUESTION 12
HOTSPOT
You have an Azure subscription that contains an Azure SQL database named SQL1.
You plan to deploy a web app named App1.
You need to provide App1 with read and write access to SQL1. The solution must meet the following requirements:
Provide App1 with access to SQL1 without storing a password.
Use the principle of least privilege. Minimize administrative effort.
Which type of account should App1 use to access SQL1, and which database roles should you assign to App1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer area

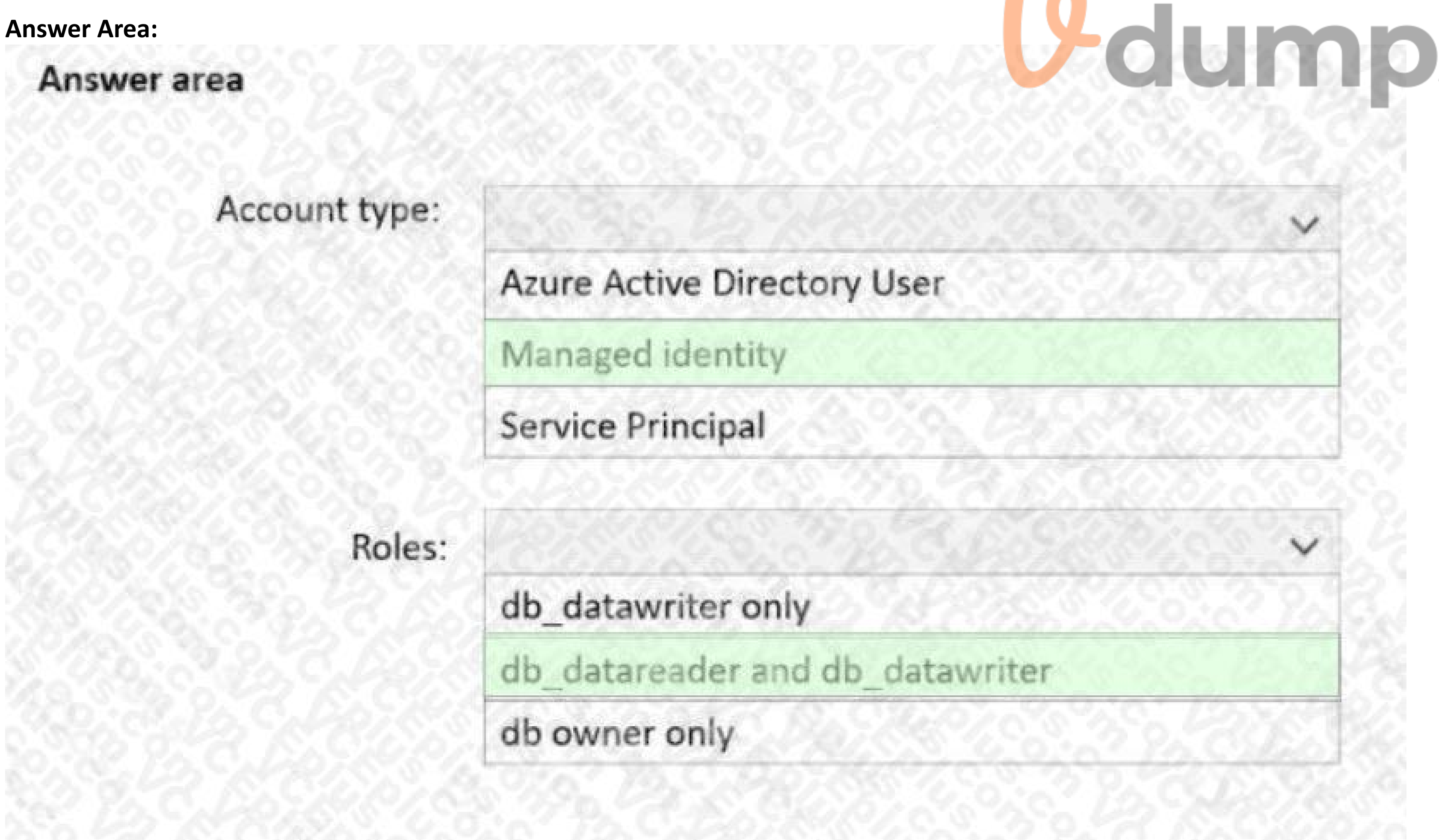
Account type:

- Azure Active Directory User
- Managed identity
- Service Principal

Roles:

- db_datawriter only
- db_datareader and db_datawriter
- db owner only

Answer Area:



Answer area

Account type:

- Azure Active Directory User
- [✓ Managed identity]
- Service Principal

Roles:

- db_datawriter only
- [✓ db_datareader and db_datawriter]
- db owner only

Section:

Explanation:
https://docs.microsoft.com/en-us/azure/app-service/tutorial-connect-msi-sql-database?tabs=windowsclient%2Cdotnet

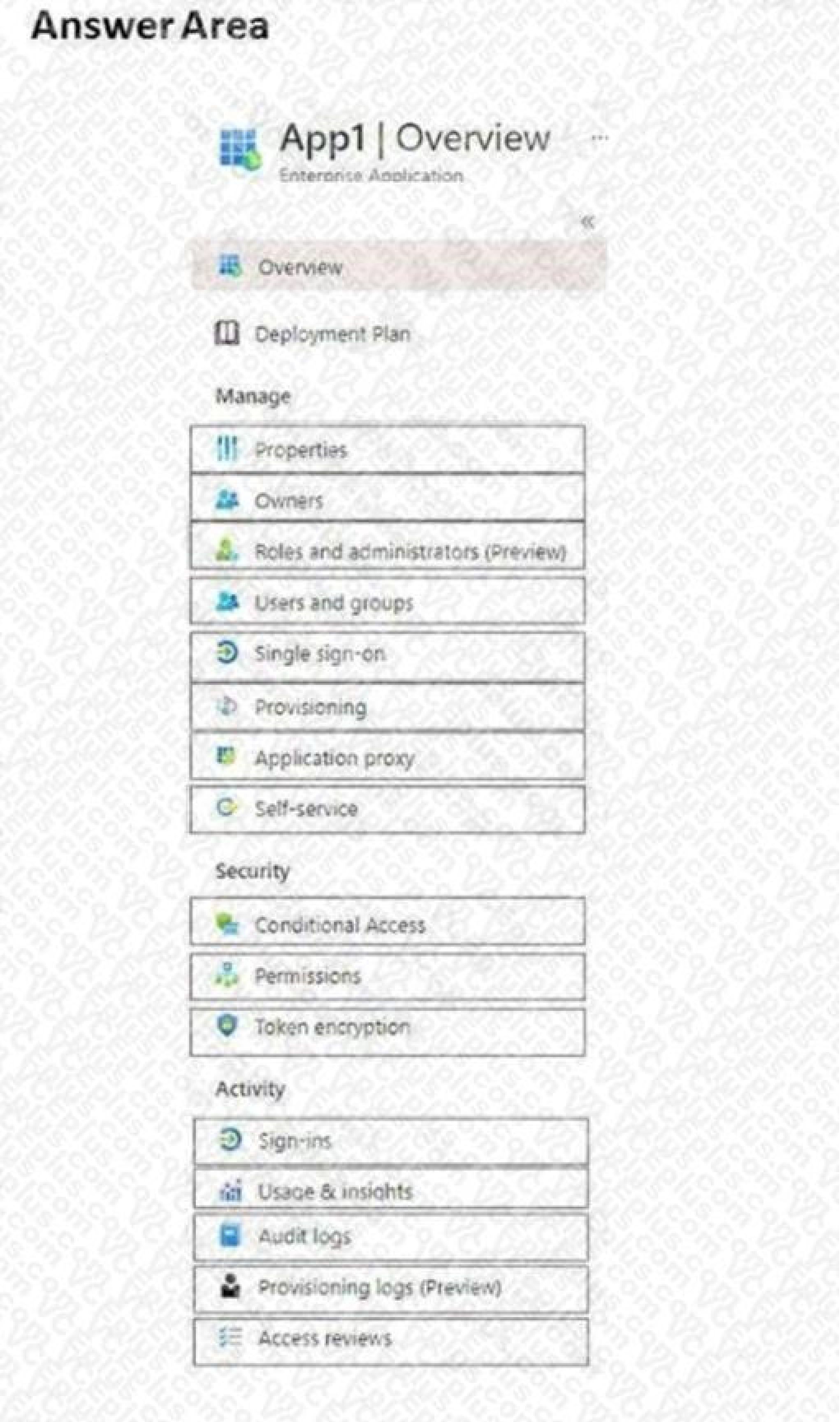
QUESTION 13

HOTSPOT

You have an Azure Active Directory (Azure AD) tenant that contains two users named User1 and User2 and a registered app named App1. You create an app-specific role named Role1.
You need to assign Role1 to User1 and enable User2 to request access to App1.
Which two settings should you modify? To answer, select the appropriate settings in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area



App1 | Overview

Enterprise Application

Overview

Deployment Plan

Manage

Properties

Owners

Roles and administrators (Preview)

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Security

Conditional Access

Permissions

Token encryption

Activity

Sign-ins

Usage & insights

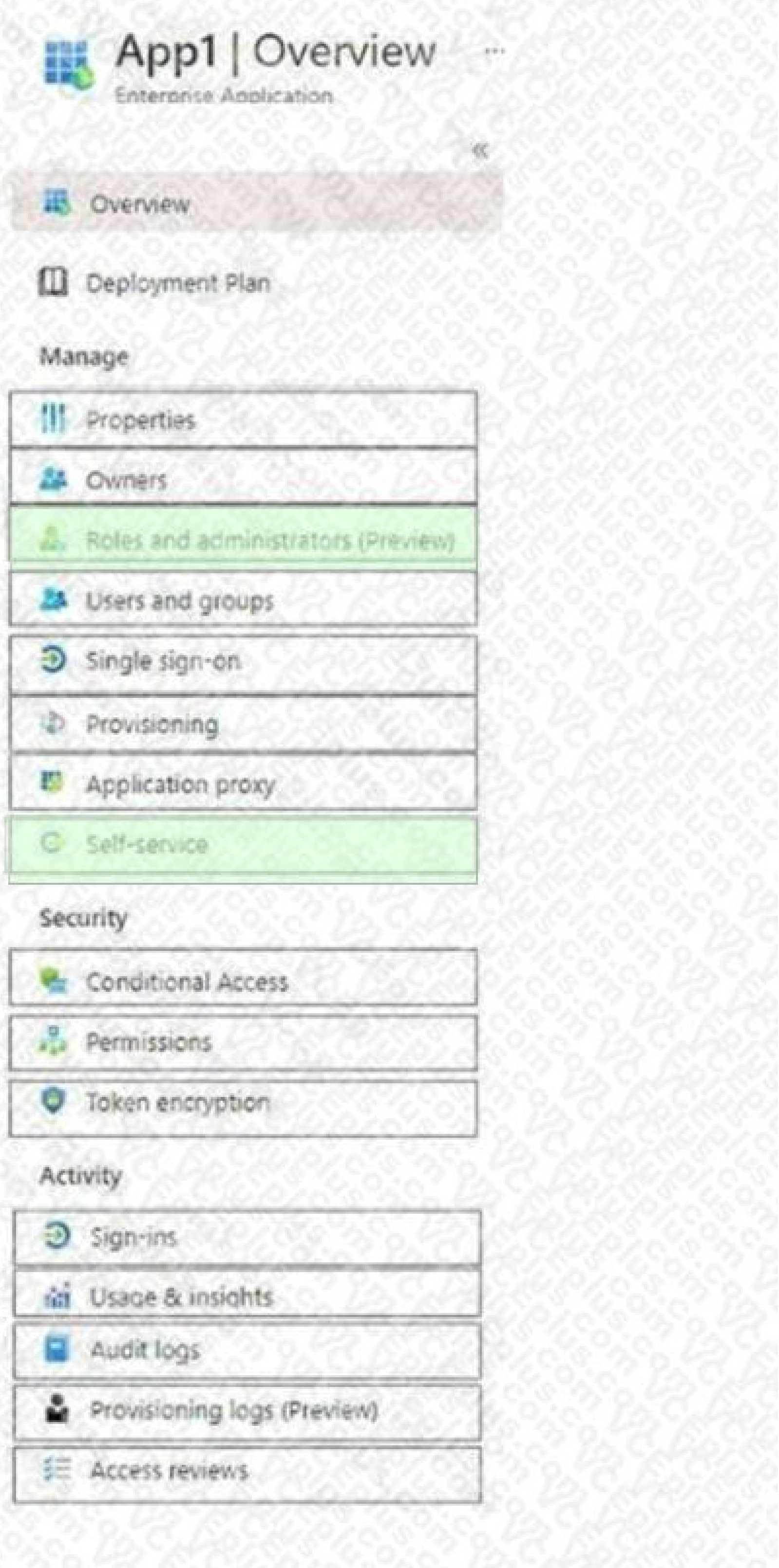
Audit logs

Provisioning logs (Preview)

Access reviews

Answer Area:

Answer Area



Section:

Explanation:

Box 1: Roles and administrators

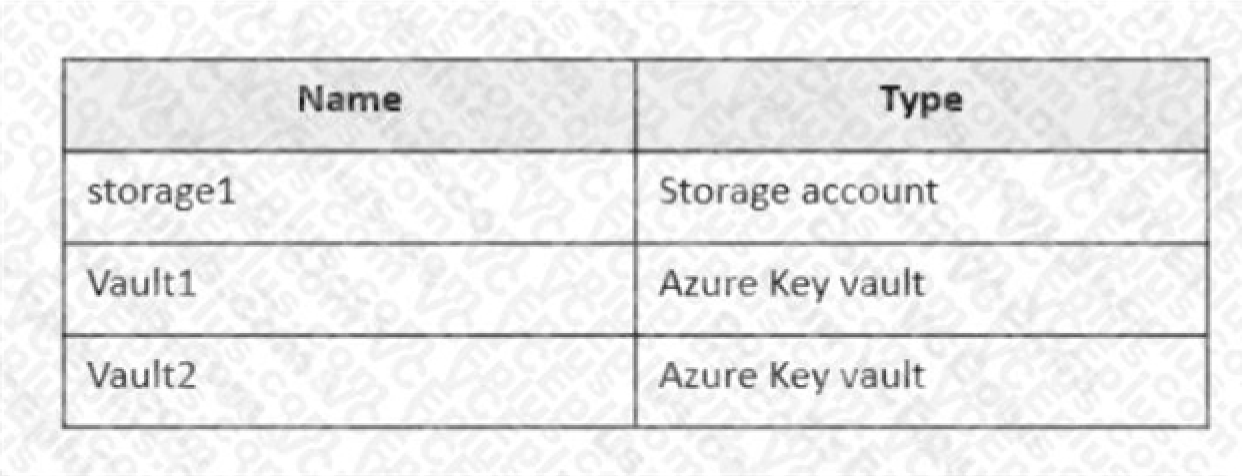
Here you will find Role1 and be able to assign User1 to the role.

Box 2: Self Service

Under Self Service, there is an option to “Allow users to request access to this application”.

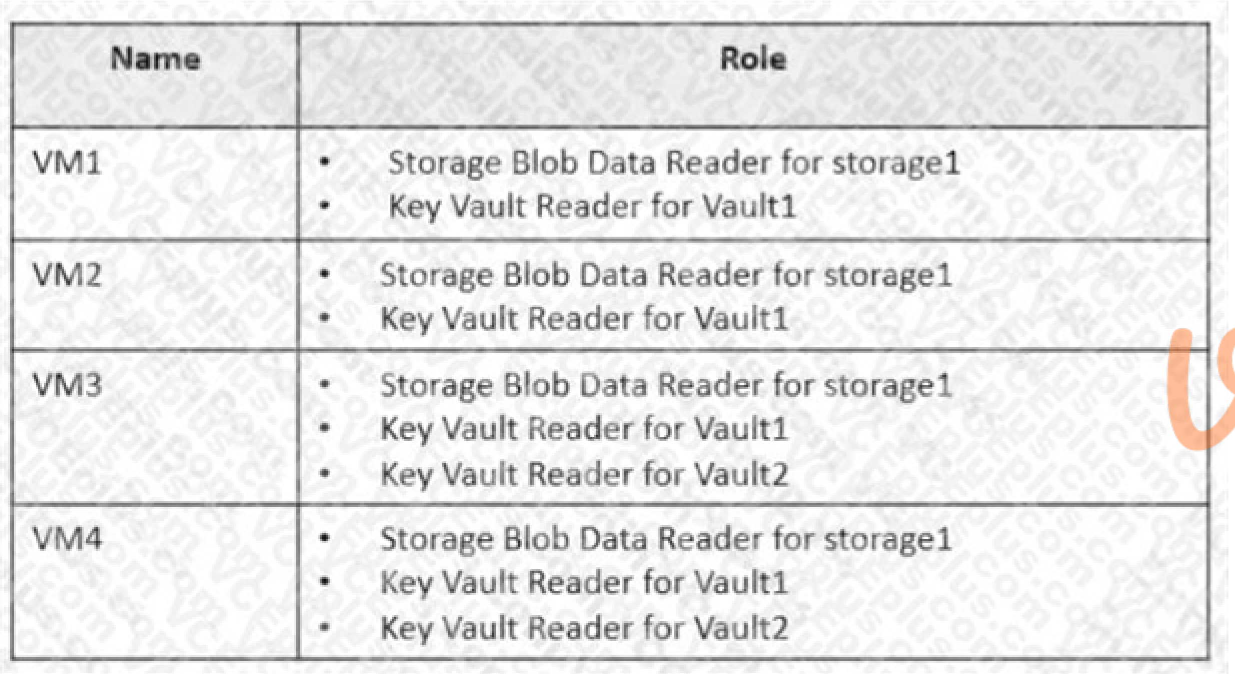
QUESTION 14

You have an Azure subscription that contains the resources shown in the following table.



Name	Type
storage1	Storage account
Vault1	Azure Key vault
Vault2	Azure Key vault

You plan to deploy the virtual machines shown in the following table.



Name	Role
VM1	• Storage Blob Data Reader for storage1 • Key Vault Reader for Vault1
VM2	• Storage Blob Data Reader for storage1 • Key Vault Reader for Vault1
VM3	• Storage Blob Data Reader for storage1 • Key Vault Reader for Vault1 • Key Vault Reader for Vault2
VM4	• Storage Blob Data Reader for storage1 • Key Vault Reader for Vault1 • Key Vault Reader for Vault2

You need to assign managed identities to the virtual machines. The solution must meet the following requirements:
Assign each virtual machine the required roles. Use the principle of least privilege.
What is the minimum number of managed identities required?

A. 1
B. 2
C. 3
D. 4

Correct Answer: B
Section:
Explanation:
We have two different sets of required permissions. VM1 and VM2 have the same permission requirements. VM3 and VM4 have the same permission requirements.
A user-assigned managed identity can be assigned to one or many resources. By using user-assigned managed identities, we can create just two managed identities: one with the permission requirements for VM1 and VM2 and the other with the permission requirements for VM3 and VM4.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

QUESTION 15

SIMULATION

You need to ensure that a user named user2-12345678 can manage the properties of the virtual machines in the RG1lod12345678 resource group. The solution must use the principle of least privilege.

To complete this task, sign in to the Azure portal.

A.

Correct Answer: A

Section:

Explanation:

Answer: A

Explanation:

1. Sign in to the Azure portal.
2. Browse to Resource Groups.
3. Select the RG1lod12345678 resource group.
4. Select Access control (IAM).
5. Select Add > role assignment.
6. Select Virtual Machine Contributor (you can filter the list of available roles by typing ‘virtual’ in the search box) then click Next.
7. Select the +Select members option and select user2-12345678 then click the Select button.
8. Click the Review + assign button twice.

Reference:

https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal?tabs=current

QUESTION 16

SIMULATION

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password. place your cursor in the Enter password box and click on the password below. Azure Username: Userl -28681041@ExamUsers.com

Azure Password: GpOAe4@lDg

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab. The following information is for technical support purposes only:

Lab Instance: 28681041

Task 10

You need to create a new Azure AD directory named 28681041.onmicrosoft.com. The new directory must contain a new user named user1@28681041.onmicrosoft.com.

A.

Correct Answer: A

Section:

Explanation:

Answer: A

Explanation:

The first step is to create the Azure Active Directory tenant.

To create a new Azure AD directory named 28681041.onmicrosoft.com that contains a new user named user1@28681041.onmicrosoft.com, you can follow these steps:

In the Azure portal, search for and select Azure Active Directory.

In the left pane, select Domains.

Select Add domain.

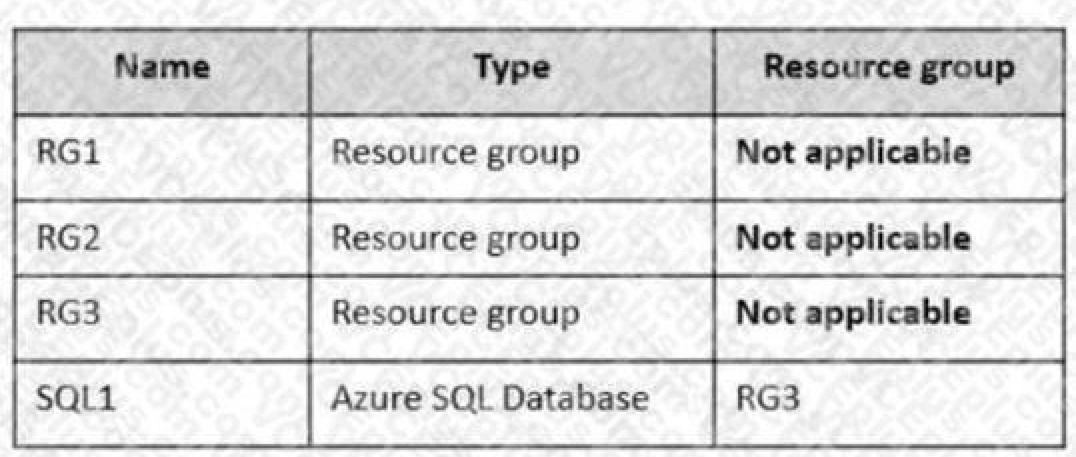
In the Add a custom domain pane, enter the following information:

Domain name: Enter the domain name you want to use. For example, 28681041.onmicrosoft.com.

Add domain: Select Add domain.

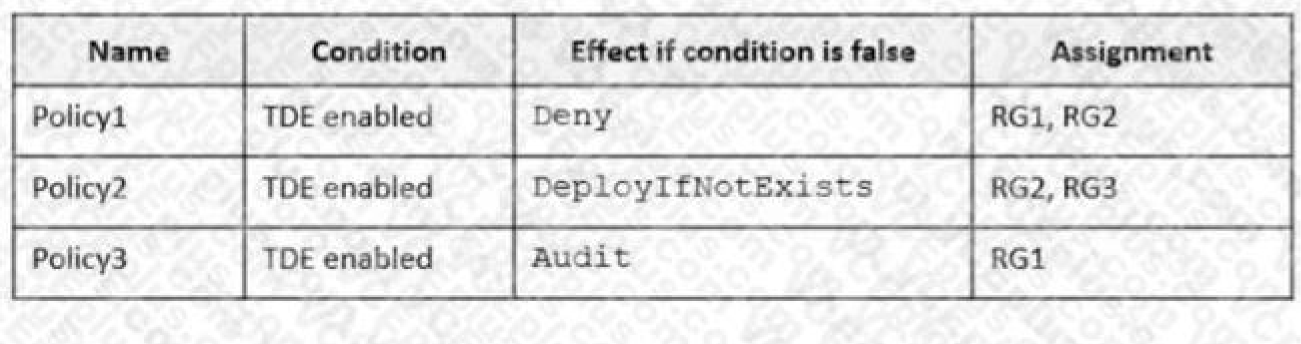
In the left pane, select Users.
Select New user.
In the New user pane, enter the following information:
User name: Enter the user name you want to use. For example, user1@28681041.onmicrosoft.com.
Name: Enter the name of the user.
Password: Enter a password for the user.
Groups: Select the groups you want the user to be a member of.
Select Create.
You can find more information on these topics in the following Microsoft documentation:
Add a custom domain name to Azure Active Directory
Create a new user in your organization - Azure Active Directory
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-access-create-new-tenant https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-users-azure-active-directory

QUESTION 17
HOTSPOT
You have an Azure subscription that contains the resources shown in the following table.



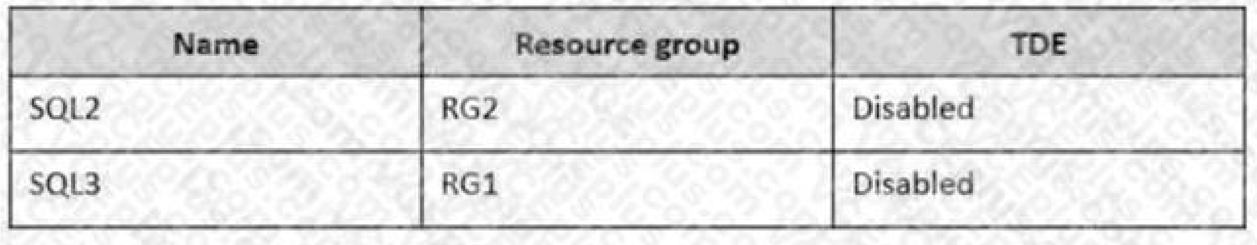
Name	Type	Resource group
RG1	Resource group	**Not applicable**
RG2	Resource group	**Not applicable**
RG3	Resource group	**Not applicable**
SQL1	Azure SQL Database	RG3

Transparent Data Encryption (TDE) is disabled on SQL1.
You assign policies to the resource groups as shown in the following table.



Name	Condition	Effect if condition is false	Assignment
Policy1	TDE enabled	`Deny`	RG1, RG2
Policy2	TDE enabled	`DeployIfNotExists`	RG2, RG3
Policy3	TDE enabled	`Audit`	RG1

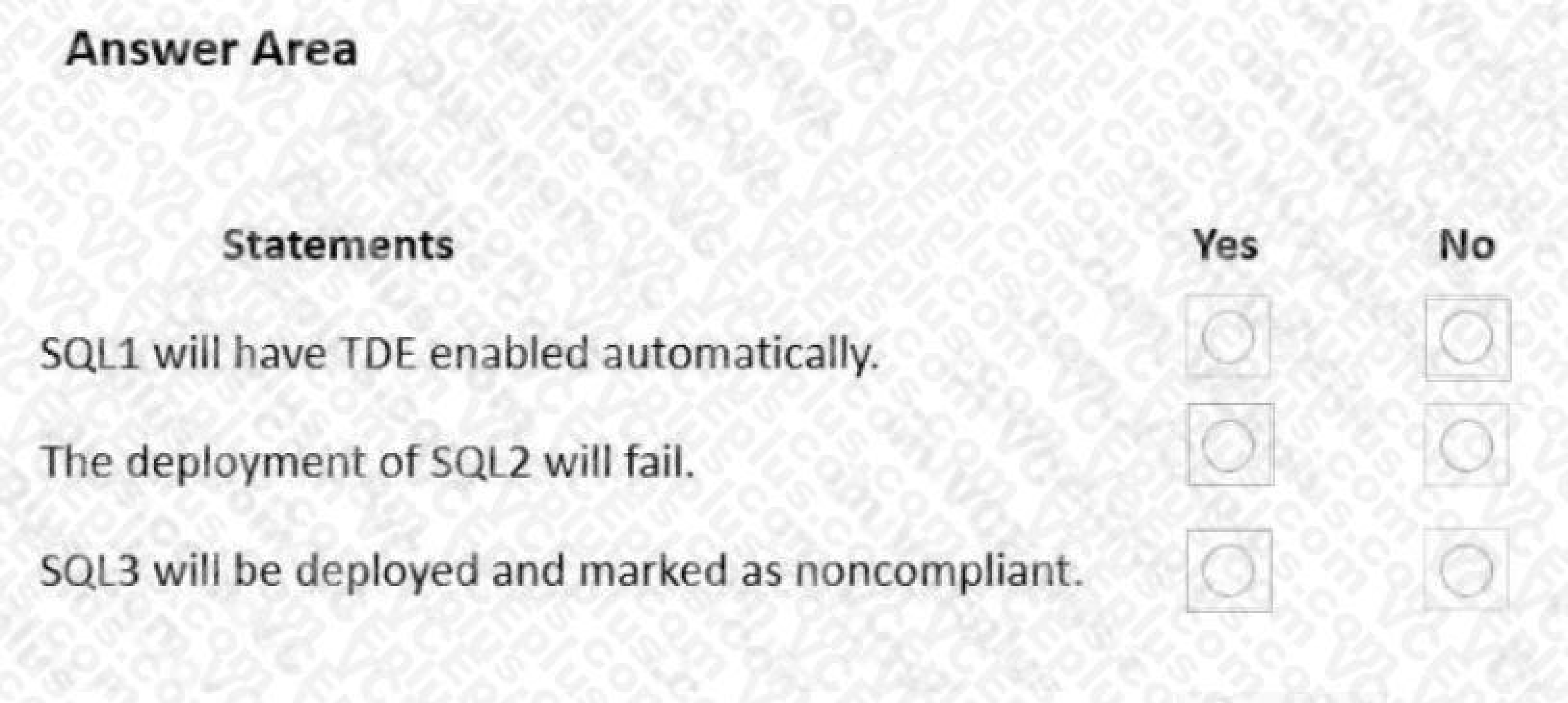
You plan to deploy Azure SQL databases by using an Azure Resource Manager (ARM) template. The databases will be configured as shown in the following table.



Name	Resource group	TDE
SQL2	RG2	Disabled
SQL3	RG1	Disabled

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

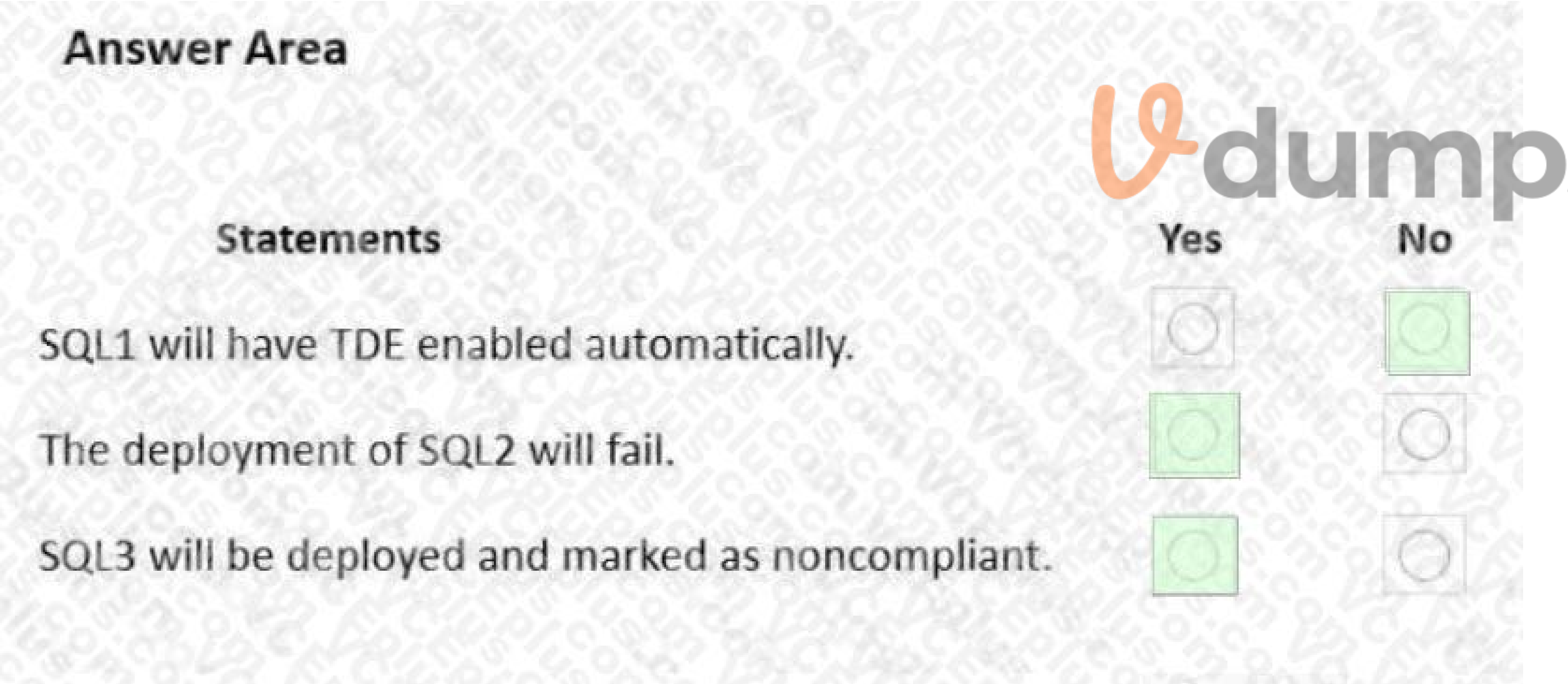
Hot Area:



Answer Area

Statements	Yes	No
SQL1 will have TDE enabled automatically.	○	○
The deployment of SQL2 will fail.	○	○
SQL3 will be deployed and marked as noncompliant.	○	○

Answer Area:

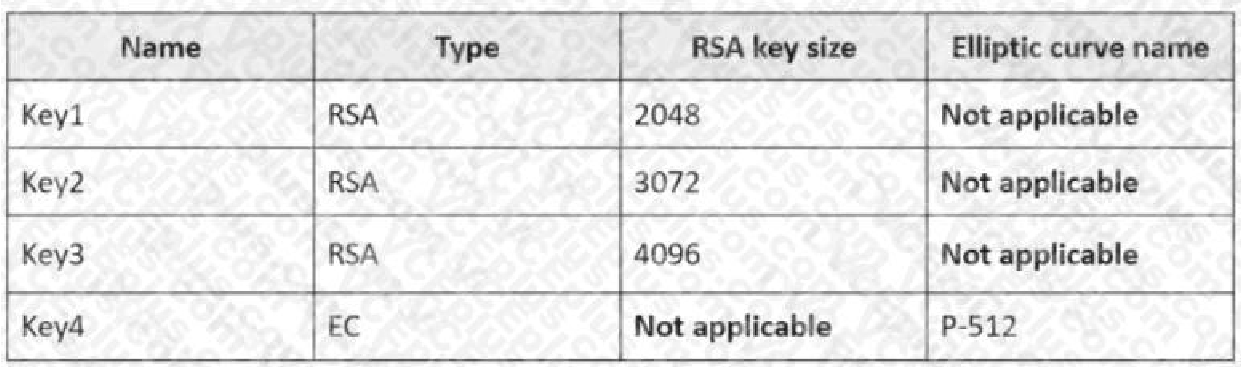


Answer Area

Statements	Yes	No
SQL1 will have TDE enabled automatically.	○	[✓ ○]
The deployment of SQL2 will fail.	[✓ ○]	○
SQL3 will be deployed and marked as noncompliant.	[✓ ○]	○

Section:
Explanation:
https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects

QUESTION 18
You have an Azure subscription that contains an Azure SQL database named SQL1 and an Azure key vault namedKeyVault1. KeyVault1 stores the keys shown in the following table. You need to configure Transparent Data Encryption (TDE). TDE will use a customer-managed key for SQL1.



Name	Type	RSA key size	Elliptic curve name
Key1	RSA	2048	Not applicable
Key2	RSA	3072	Not applicable
Key3	RSA	4096	Not applicable
Key4	EC	Not applicable	P-512

Which keys can you use?

A. Key2 only
B. Key1 only
C. Key2 and Key3 only
D. Key1, Key2, Key3, and Key4
E. Key1 and Key2 only

Correct Answer: E
Section:
Explanation:
The key must be an asymmetric, RSA or RSA HSM key. The supported key lengths are 2048-bit and 3072-bit.
Reference:
https://docs.microsoft.com/en-us/azure/azure-sql/database/transparent-data-encryption-byok-overview

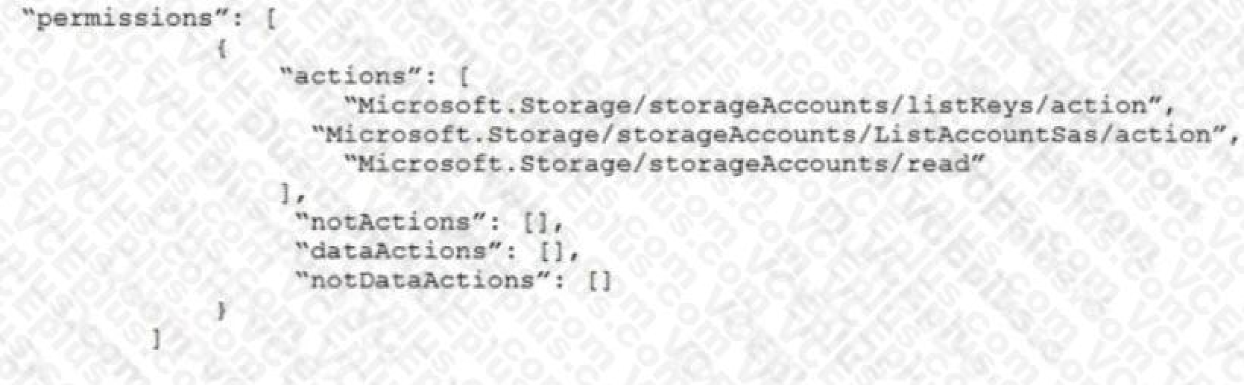
QUESTION 19
SIMULATION
You need to create a web app named Intranet12345678 and enable users to authenticate to the web app by using Azure Active Directory (Azure AD). To complete this task, sign in to the Azure portal.

A.

Correct Answer: A
Section:
Explanation:
Answer: A
Explanation:
1. In the Azure portal, type App services in the search box and select App services from the search results. 2. Click the Create app service button to create a new app service.
3. In the Resource Group section, click the Create new link to create a new resource group.
4. Give the resource group a name such as Intranet12345678RG and click OK.
5. In the Instance Details section, enter Intranet12345678 in the Name field.
6. In the Runtime stack field, select any runtime stack such as .NET Core 3.1.
7. Click the Review + create button.
8. Click the Create button to create the web app.
9. Click the Go to resource button to open the properties of the new web app.
10.In the Settings section, click on Authentication / Authorization.
11.Click the App Service Authentication slider to set it to On.
12.In the Action to take when request is not authentication box, select Log in with Azure Active Directory. 13.Click Save to save the changes.

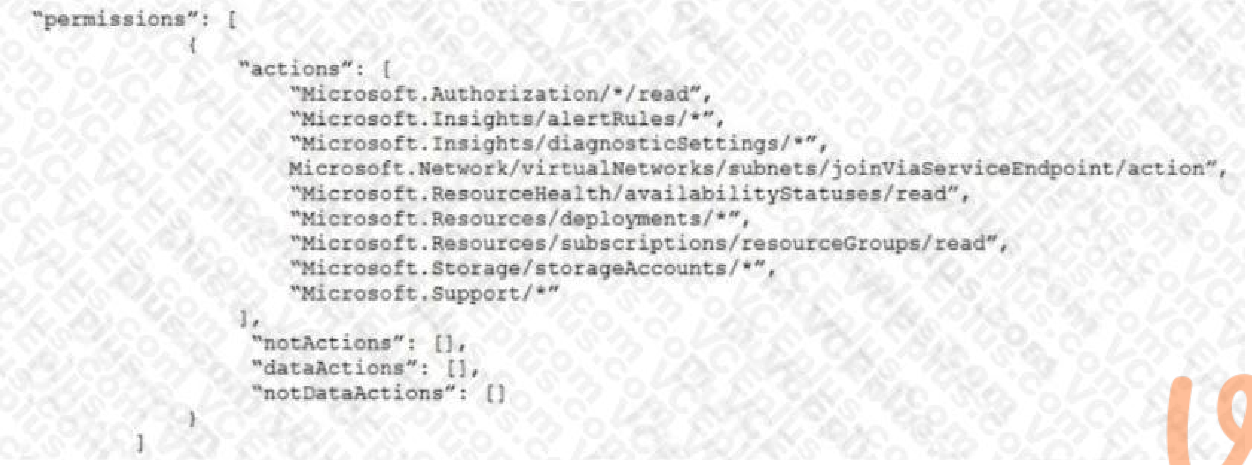
QUESTION 20
HOTSPOT

You have an Azure subscription that contains a resource group named RG1. RG1 contains a storage account named storage1.
You have two custom Azure roles named Role1 and Role2 that are scoped to RG1.
The permissions for Role1 are shown in the following JSON code.



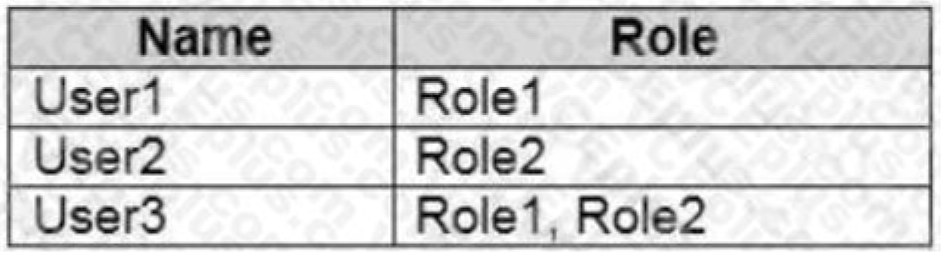
```
 "permissions": [
            {
                "actions": [
                    "Microsoft.Storage/storageAccounts/listKeys/action",
                  "Microsoft.Storage/storageAccounts/ListAccountSas/action",
                    "Microsoft.Storage/storageAccounts/read"
                ],
                 "notActions": [],
                 "dataActions": [],
                 "notDataActions": []
            }
        ]
```

The permissions for Role2 are shown in the following JSON code.



```
  "permissions": [
            {
                "actions": [
                    "Microsoft.Authorization/*/read",
                    "Microsoft.Insights/alertRules/*",
                    "Microsoft.Insights/diagnosticSettings/*",
                    Microsoft.Network/virtualNetworks/subnets/joinViaServiceEndpoint/action",
                    "Microsoft.ResourceHealth/availabilityStatuses/read",
                    "Microsoft.Resources/deployments/*",
                    "Microsoft.Resources/subscriptions/resourceGroups/read",
                    "Microsoft.Storage/storageAccounts/*",
                    "Microsoft.Support/*"
                ],
                 "notActions": [],
                 "dataActions": [],
                 "notDataActions": []
            }
        ]
```

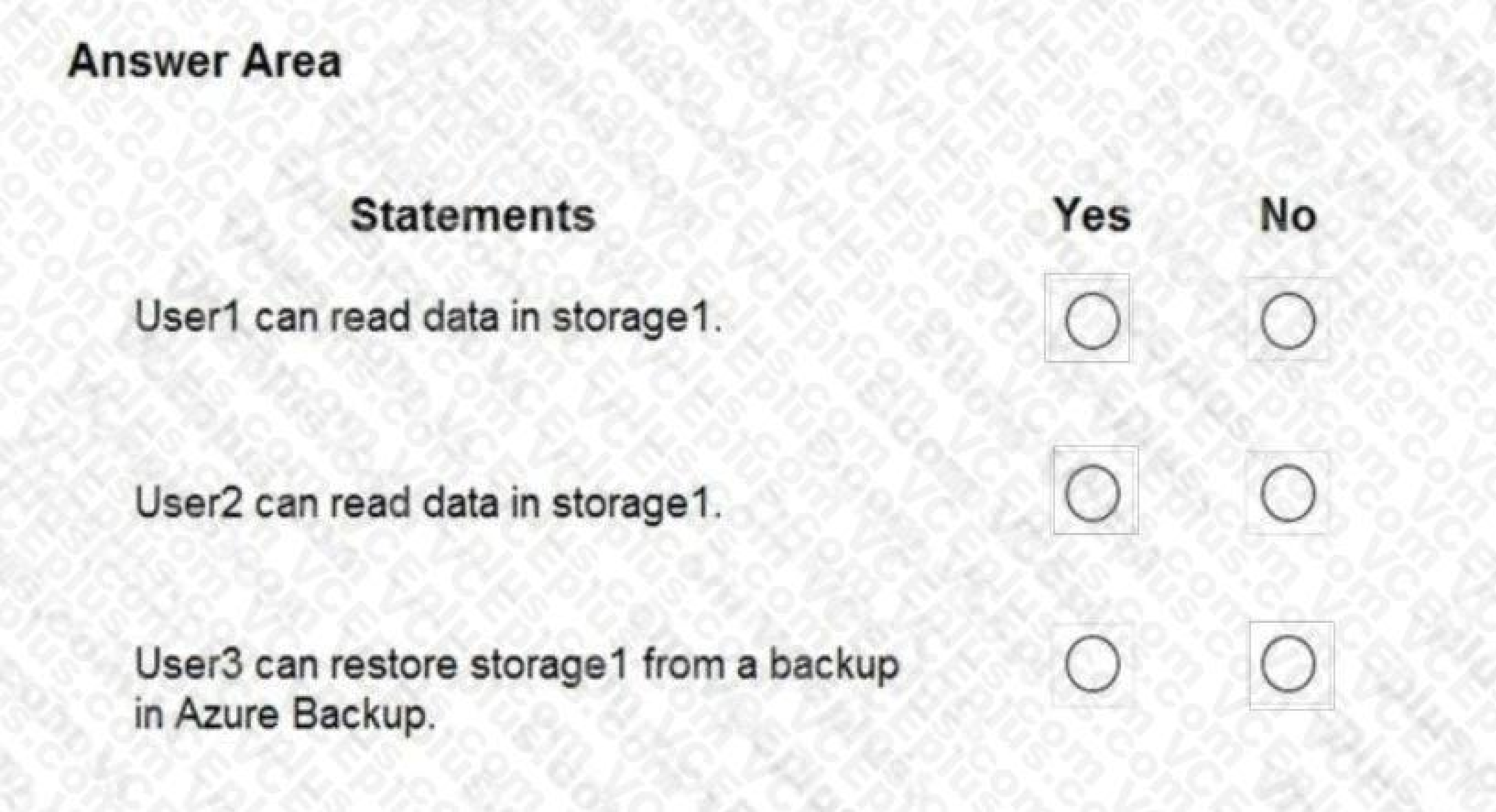
You assign the roles to the users shown in the following table.



Name	Role
User1	Role1
User2	Role2
User3	Role1, Role2

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

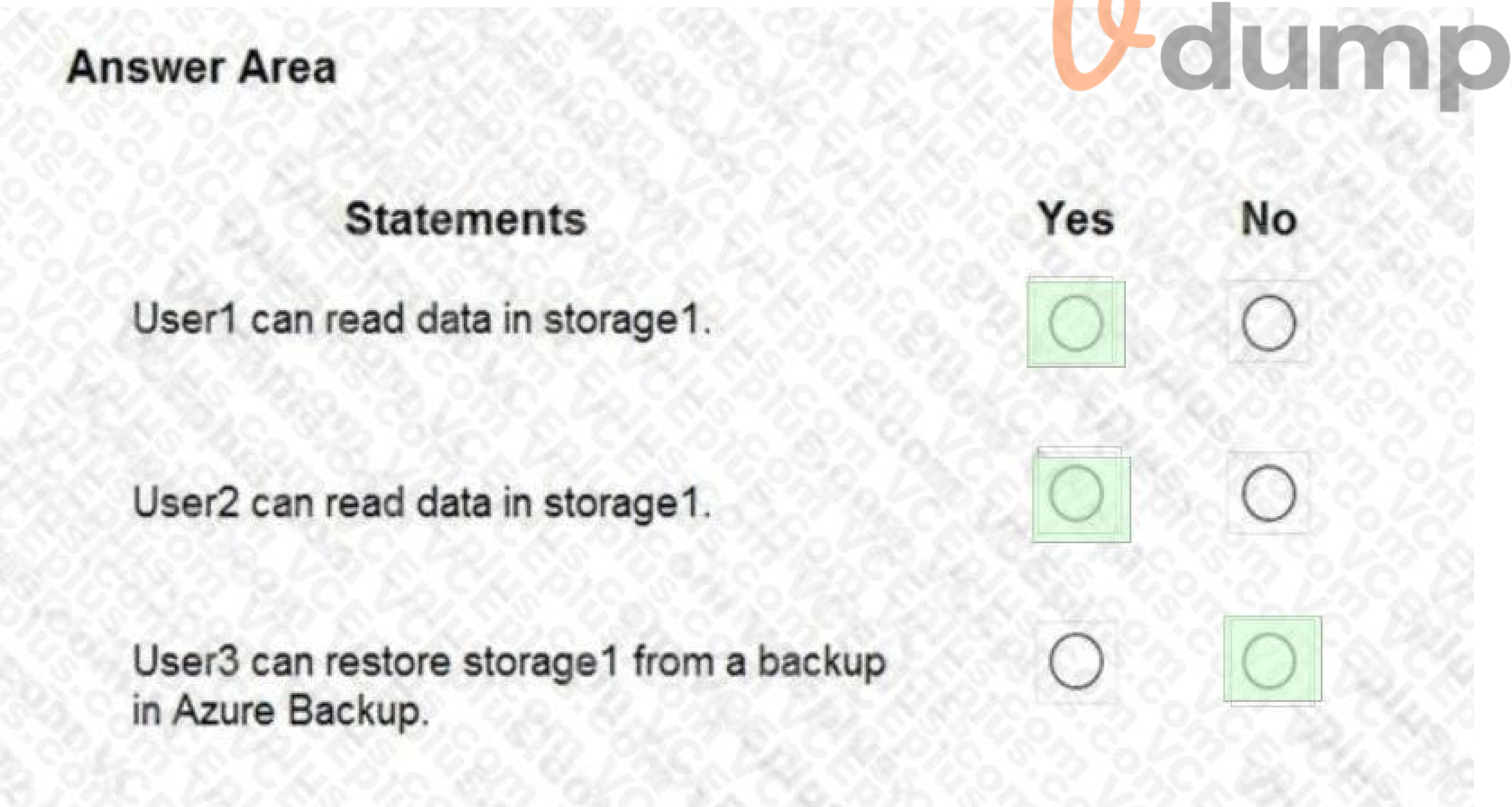
Hot Area:



Answer Area

Statements	Yes	No
User1 can read data in storage1.	○	○
User2 can read data in storage1.	○	○
User3 can restore storage1 from a backup in Azure Backup.	○	○

Answer Area:



Answer Area

Statements	Yes	No
User1 can read data in storage1.	[✓ ○]	○
User2 can read data in storage1.	[✓ ○]	○
User3 can restore storage1 from a backup in Azure Backup.	○	[✓ ○]

Section:

Explanation:

Reference: https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles

QUESTION 21
You are troubleshooting a security issue for an Azure Storage account.
You enable Azure Storage Analytics logs and archive it to a storage account.
What should you use to retrieve the diagnostics logs?

A. Azure Cosmos DB explorer
B. SQL query editor in Azure
C. AzCopy
D. the Security admin center

Correct Answer: C
Section:

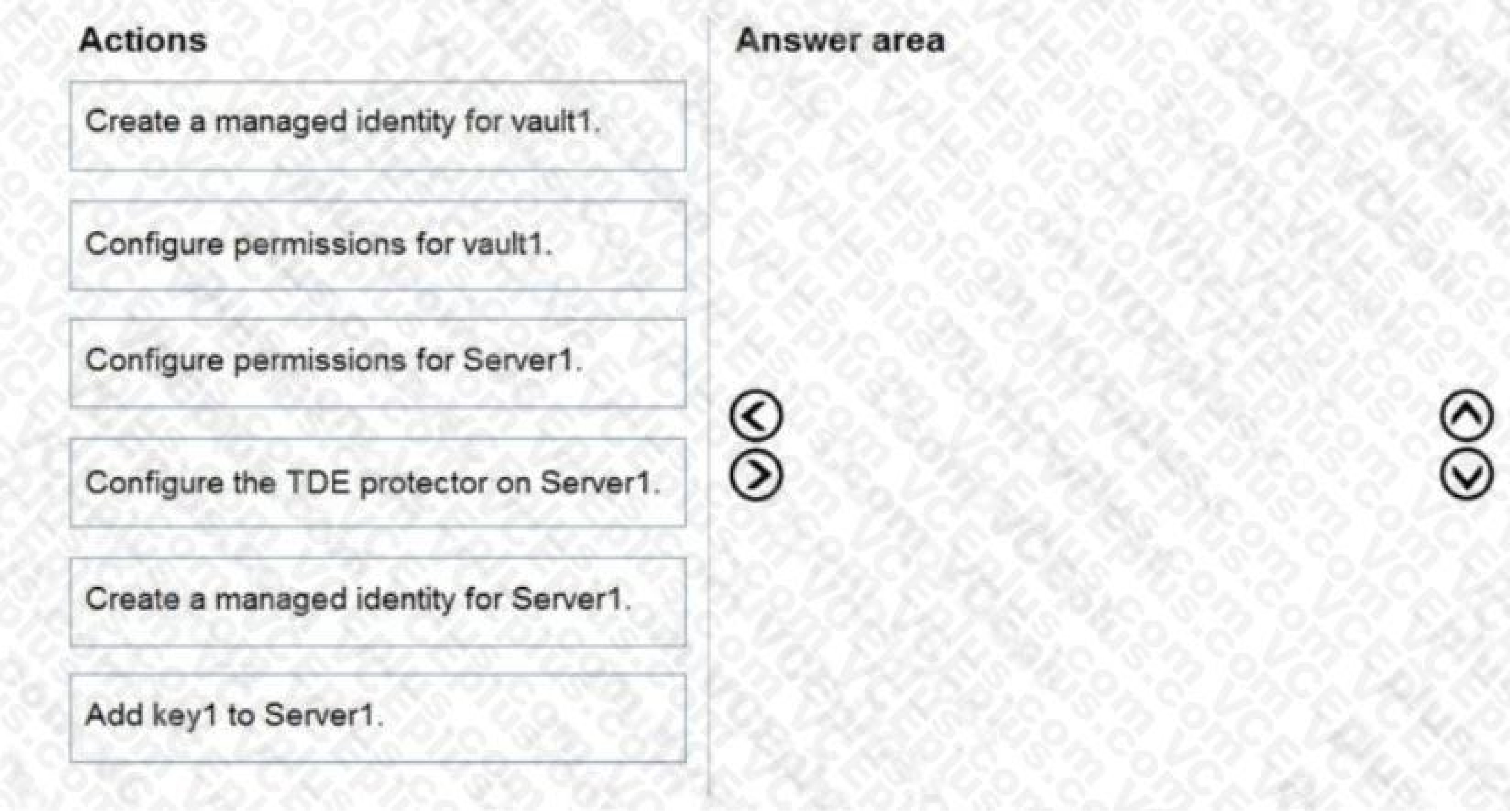
QUESTION 22
You have an Azure Sentinel workspace.
You need to create a playbook.
Which two triggers will start the playbook? Each correct answer presents a complete solution, NOTE: Each correct selection is worth one point.

A. An Azure Sentinel scheduled query rule is executed.
B. An Azure Sentinel data connector is added.
C. An Azure Sentinel alert is generated.
D. An Azure Sentinel hunting query result is returned.
E. An Azure Sentinel incident is created.

Correct Answer: C, E
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

QUESTION 23
DRAG DROP
You have an Azure subscription that contains a Microsoft SQL server named Server1 and an Azure key vault named vault1. Server1 hosts a database named DB1. Vault1 contains an encryption key named key1.
You need to ensure that you can enable Transparent Data Encryption (TDE) on DB1 by using key1.
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Actions

Create a managed identity for vault1.

Configure permissions for vault1.

Configure permissions for Server1.

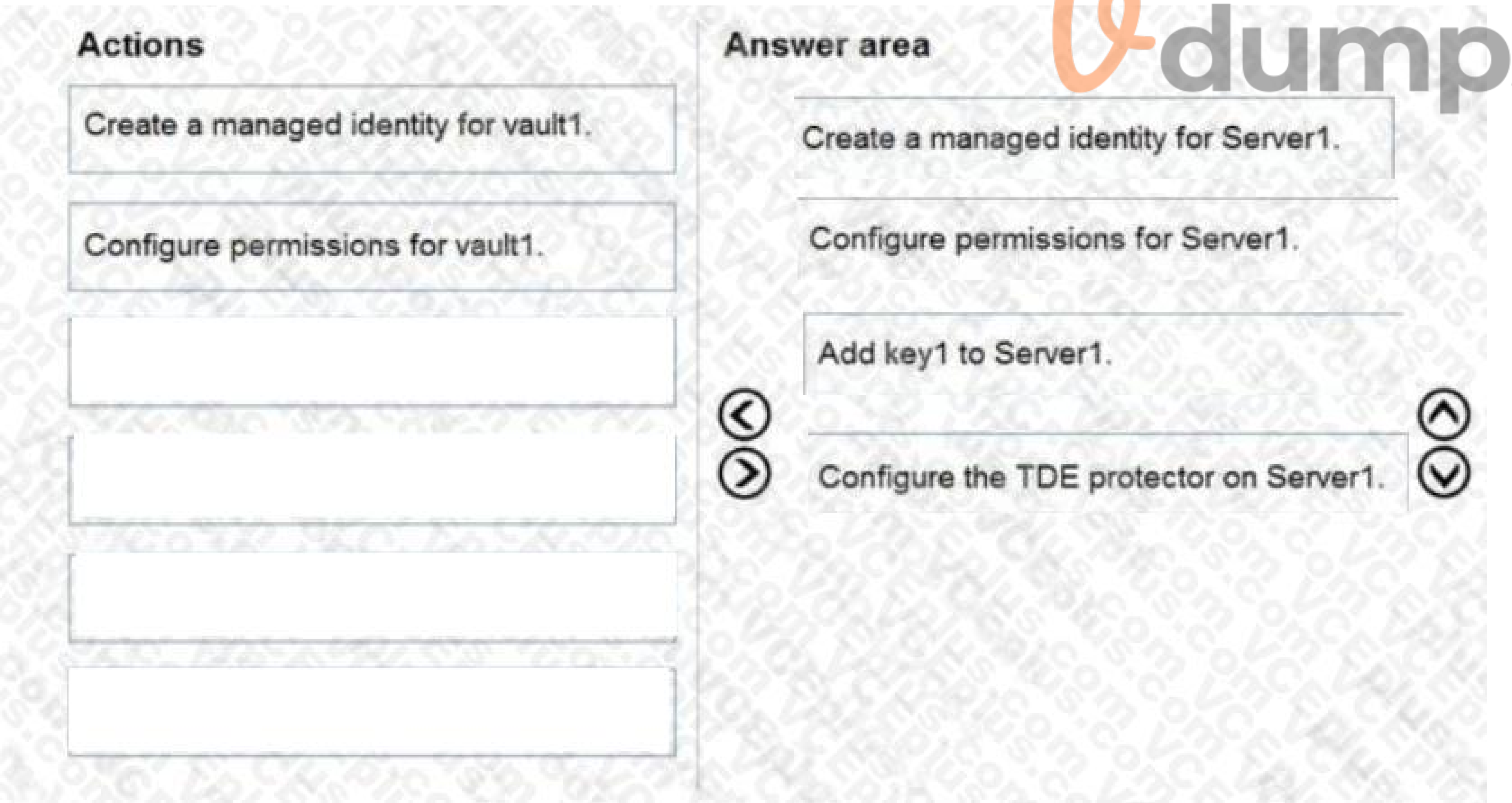
Configure the TDE protector on Server1.

Create a managed identity for Server1.

Add key1 to Server1.

Answer area

Correct Answer:



Actions

Create a managed identity for vault1.

Configure permissions for vault1.

Answer area

Create a managed identity for Server1.

Configure permissions for Server1.

Add key1 to Server1.

Configure the TDE protector on Server1.

Section:

Explanation:

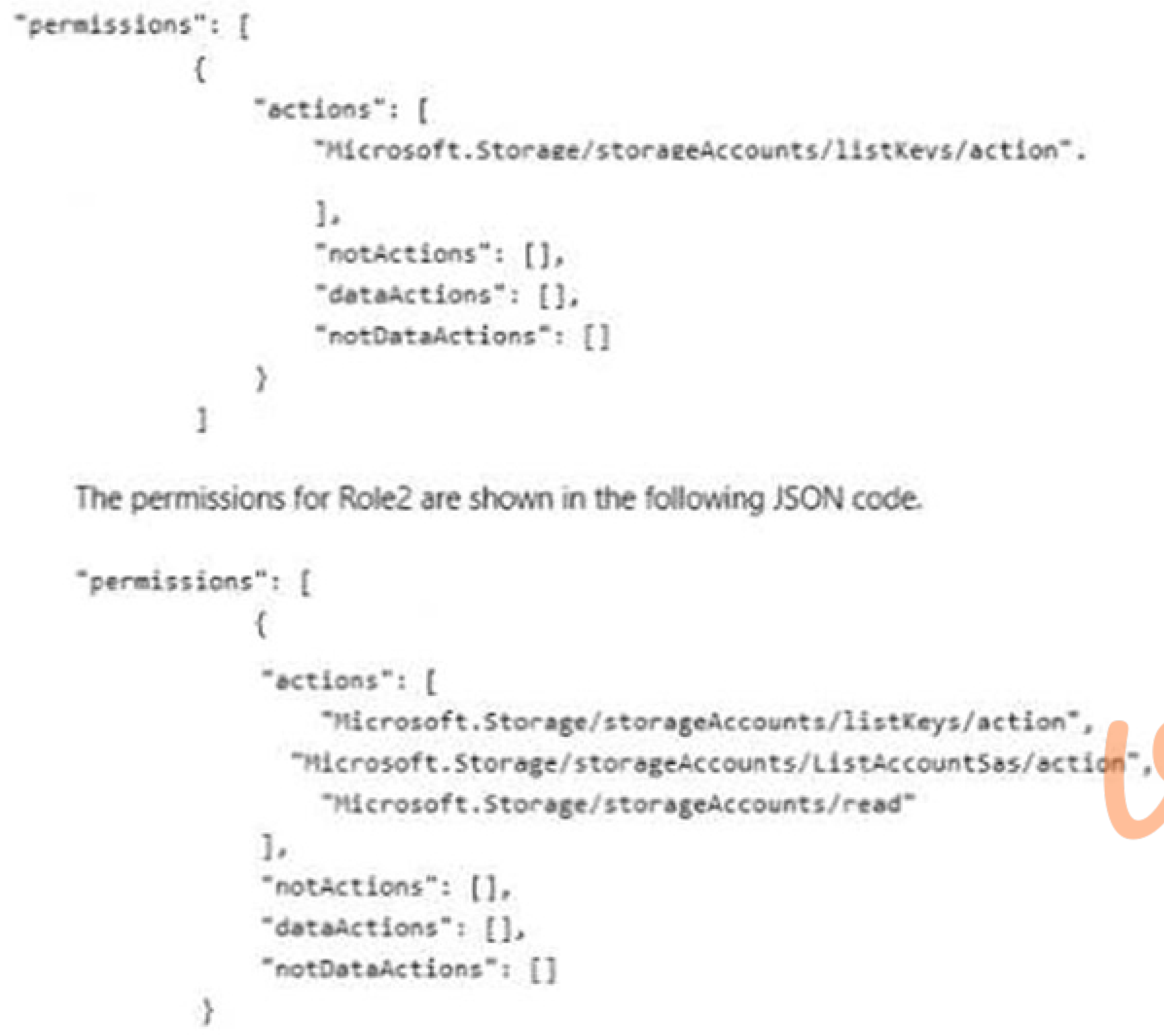
Reference: https://docs.microsoft.com/en-us/azure/azure-sql/database/transparent-data-encryption-byok-configure?tabs=azure-powershell

QUESTION 24

HOTSPOT

You have an Azure subscription mat contains a resource group named RG1. RG1 contains a storage account named storage1. You have two custom Azure rotes named Role1 and Role2 that are scoped to RG1.

The permissions for Role1 are shown in the following JSON code.



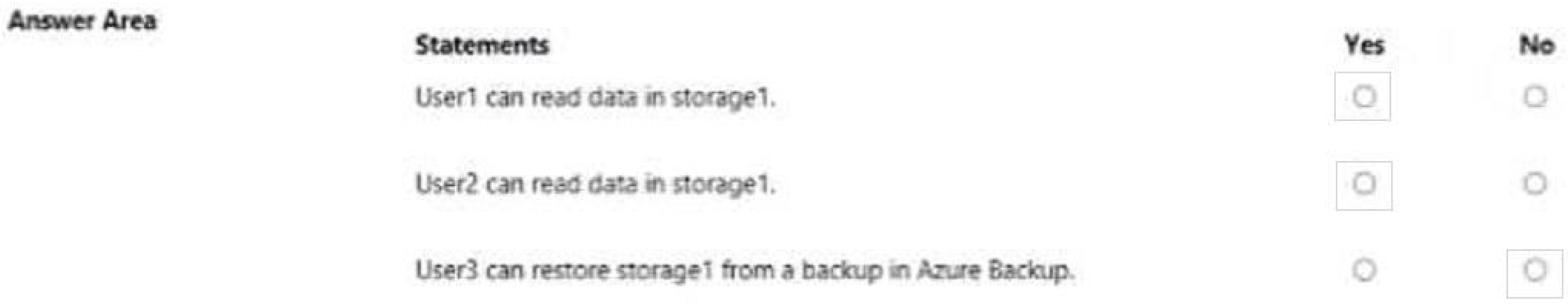
```
"permissions": [
            {
                "actions": [
                    "Microsoft.Storage/storageAccounts/listKeys/action".

                    ],
                    "notActions": [],
                    "dataActions": [],
                    "notDataActions": []
                }
            ]
```

The permissions for Role2 are shown in the following JSON code.

```
"permissions": [
            {
            "actions": [
                "Microsoft.Storage/storageAccounts/listKeys/action",
              "Microsoft.Storage/storageAccounts/ListAccountSas/action",
                "Microsoft.Storage/storageAccounts/read"
            ],
            "notActions": [],
            "dataActions": [],
            "notDataActions": []
        }
```

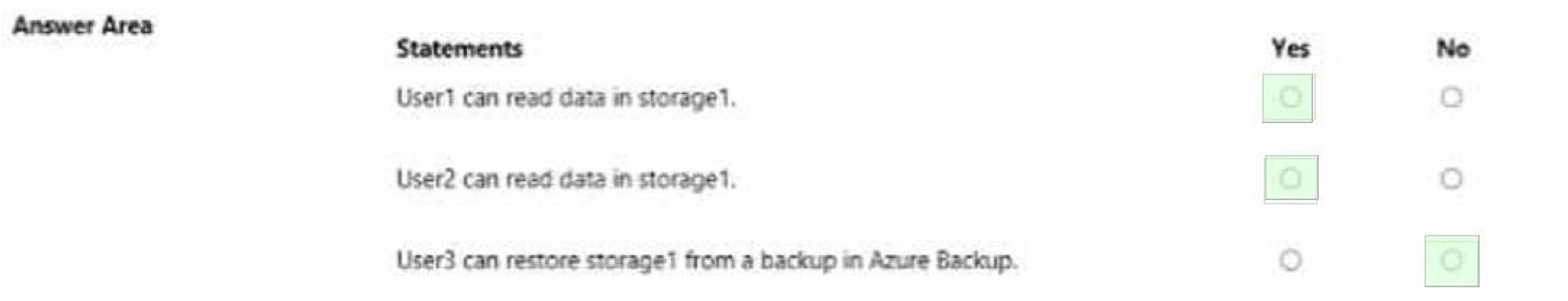
Hot Area:



Answer Area

Statements	Yes	No
User1 can read data in storage1.	○	○
User2 can read data in storage1.	○	○
User3 can restore storage1 from a backup in Azure Backup.	○	○

Answer Area:

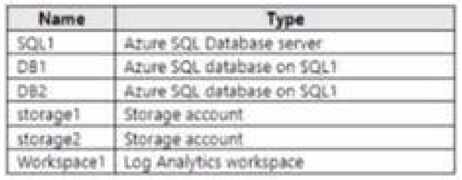


Answer Area

Statements	Yes	No
User1 can read data in storage1.	[✓ ○]	○
User2 can read data in storage1.	[✓ ○]	○
User3 can restore storage1 from a backup in Azure Backup.	○	[✓ ○]

Section:
Explanation:

QUESTION 25
HOTSPOT
You have an Azure subscription that contains the resources shown in the following table.



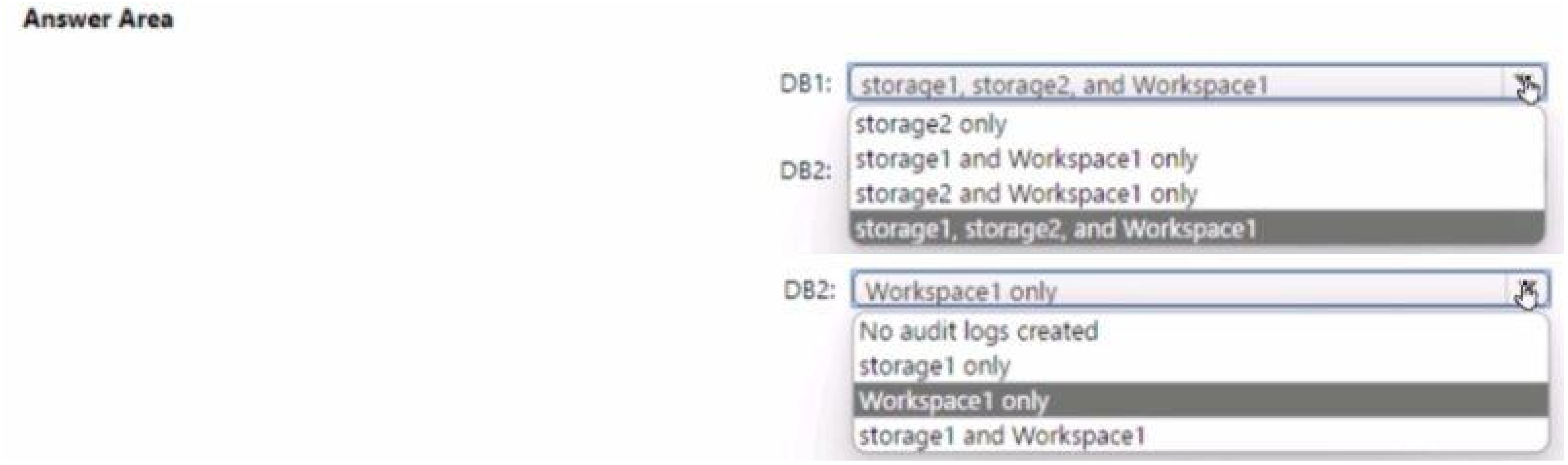
Name	Type
SQL1	Azure SQL Database server
DB1	Azure SQL database on SQL1
DB2	Azure SQL database on SQL1
storage1	Storage account
storage2	Storage account
Workspace1	Log Analytics workspace

SQL1 has the following configurations:
- Auditing: Enabled
- Audit log destination: storage1, Workspace1

DB1 has the following configurations:
- Auditing: Enabled
- Audit log destination: storage2

DB2 has auditing disabled.
Where are the audit logs for DB1 and DB2 stored? To answer, select the appropriate options in the answer area NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

DB1: storage1, storage2, and Workspace1

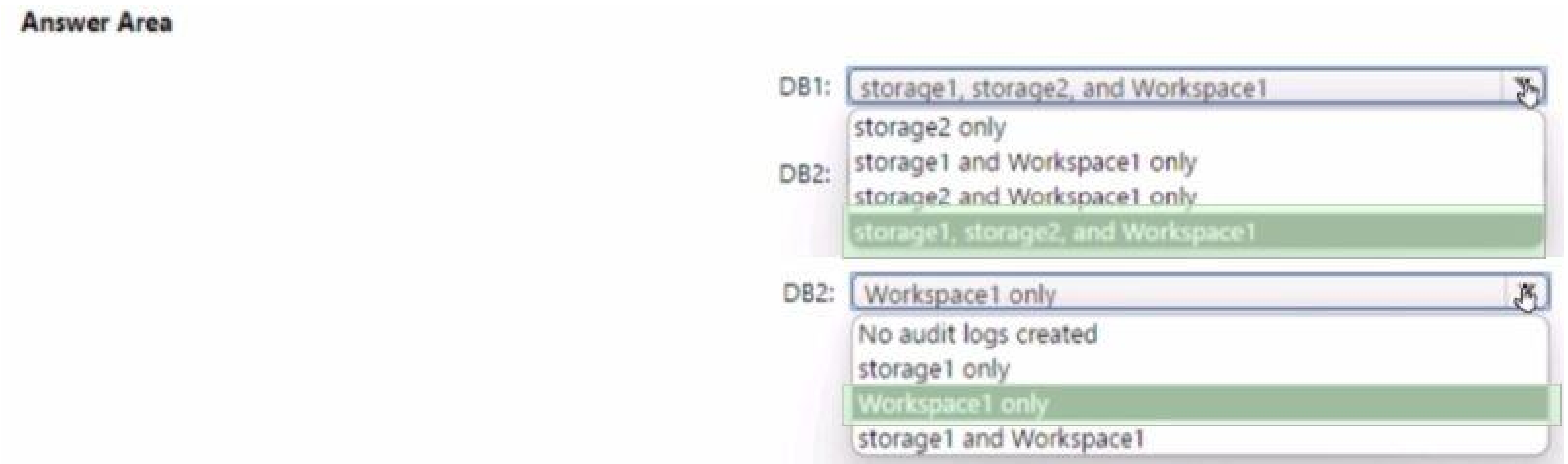
- storage2 only
- storage1 and Workspace1 only
- storage2 and Workspace1 only
- storage1, storage2, and Workspace1

DB2:

DB2: Workspace1 only

- No audit logs created
- storage1 only
- Workspace1 only
- storage1 and Workspace1

Answer Area:



Answer Area

DB1: storage1, storage2, and Workspace1

- storage2 only
- storage1 and Workspace1 only
- storage2 and Workspace1 only
- storage1, storage2, and Workspace1

DB2:

DB2: Workspace1 only

- No audit logs created
- storage1 only
- Workspace1 only
- storage1 and Workspace1

Section:
Explanation:

QUESTION 26

HOTSPOT

You have an Azure subscription that contains the virtual machines shown in the following table.

Subnet1 and Subnet2 have a network security group {NSG). The NSG has an outbound rule that has the following configurations:

- Port; Any
- Source: Any
- Priority: 100
- Action: Deny
- Protocol: Any
- Destination: Storage

The subscription contains a storage account named storage1.

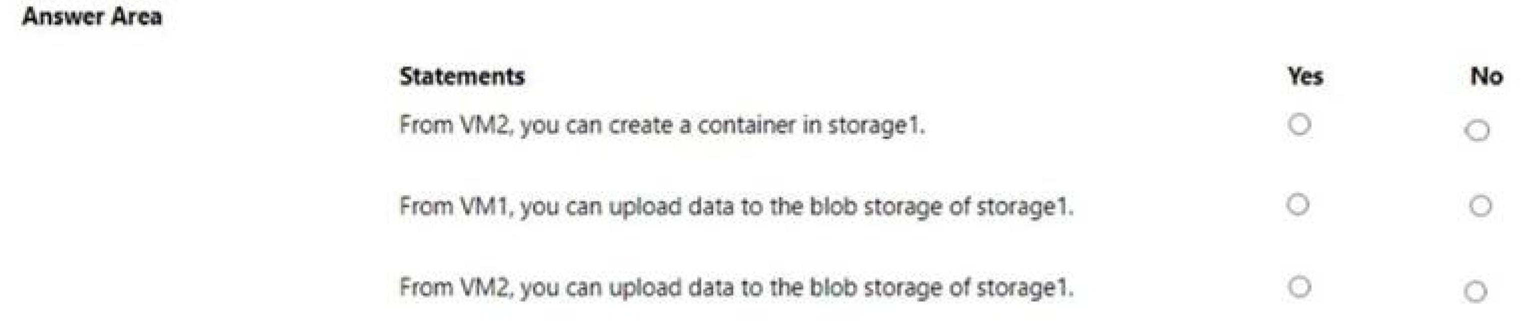
You create a private endpoint named Private1 that has the following settings:

- Resource type: Microsoft.Storage/storageAccounts
- Resource: storage1
- Target sub-resource: blob
- Virtual network: VNet1
- Subnet: Subnet1

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

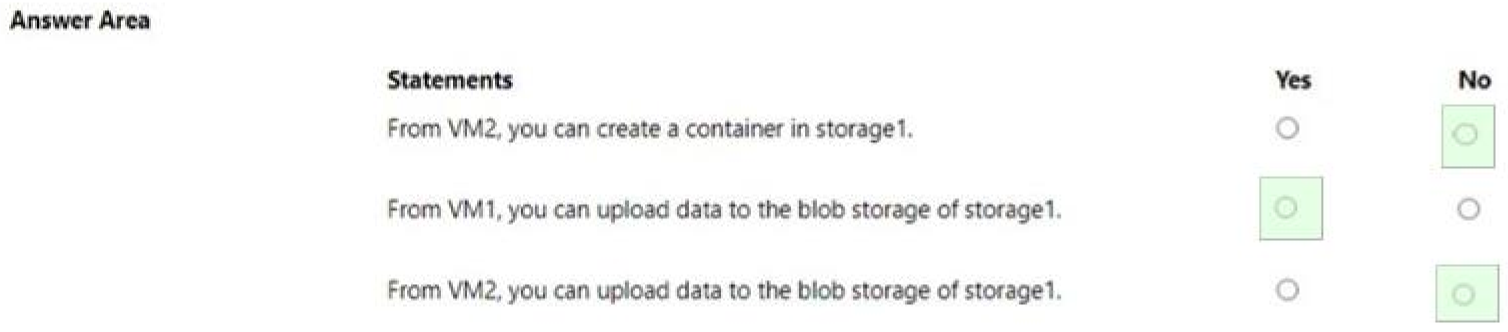
Hot Area:



Answer Area

Statements	Yes	No
From VM2, you can create a container in storage1.	○	○
From VM1, you can upload data to the blob storage of storage1.	○	○
From VM2, you can upload data to the blob storage of storage1.	○	○

Answer Area:

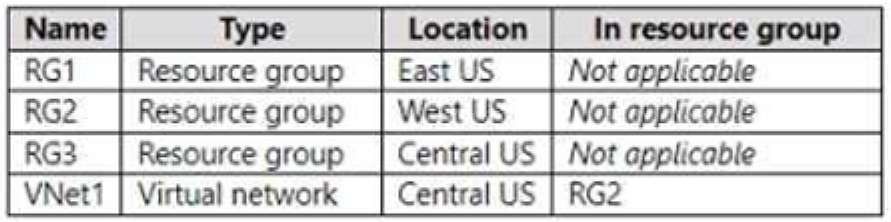


Answer Area

Statements	Yes	No
From VM2, you can create a container in storage1.	○	[✓ ○]
From VM1, you can upload data to the blob storage of storage1.	[✓ ○]	○
From VM2, you can upload data to the blob storage of storage1.	○	[✓ ○]

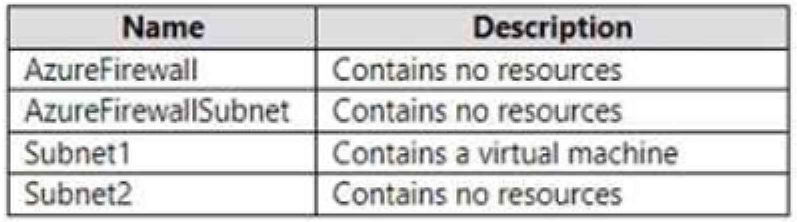
Section:
Explanation:

QUESTION 27
HOTSPOT
You have an Azure subscription that contains the resources shown in the following table.



Name	Type	Location	In resource group
RG1	Resource group	East US	*Not applicable*
RG2	Resource group	West US	*Not applicable*
RG3	Resource group	Central US	*Not applicable*
VNet1	Virtual network	Central US	RG2

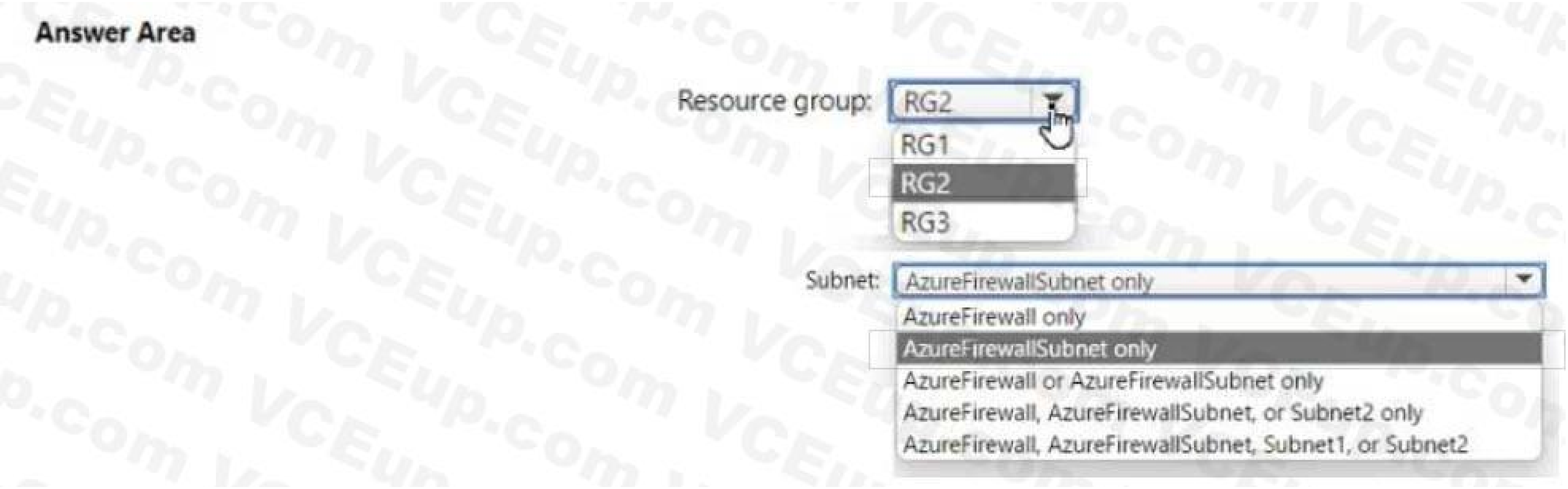
VNet1 contains the subnets shown in the following table.



Name	Description
AzureFirewall	Contains no resources
AzureFirewallSubnet	Contains no resources
Subnet1	Contains a virtual machine
Subnet2	Contains no resources

You plan to use the Azure portal to deploy an Azure firewall named AzFW1 to VNet1.
Which resource group and subnet can you use to deploy AzFW1? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:



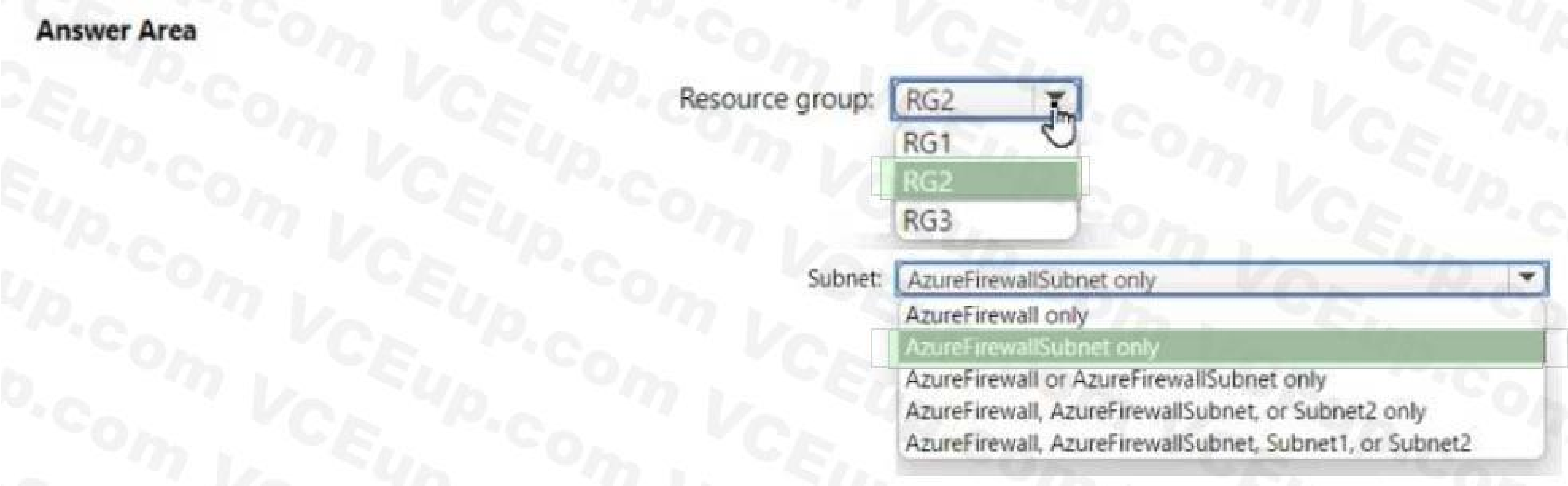
Answer Area

Resource group: RG2

Subnet: AzureFirewallSubnet only

AzureFirewall only
AzureFirewallSubnet only
AzureFirewall or AzureFirewallSubnet only
AzureFirewall, AzureFirewallSubnet, or Subnet2 only
AzureFirewall, AzureFirewallSubnet, Subnet1, or Subnet2

Answer Area:



Answer Area

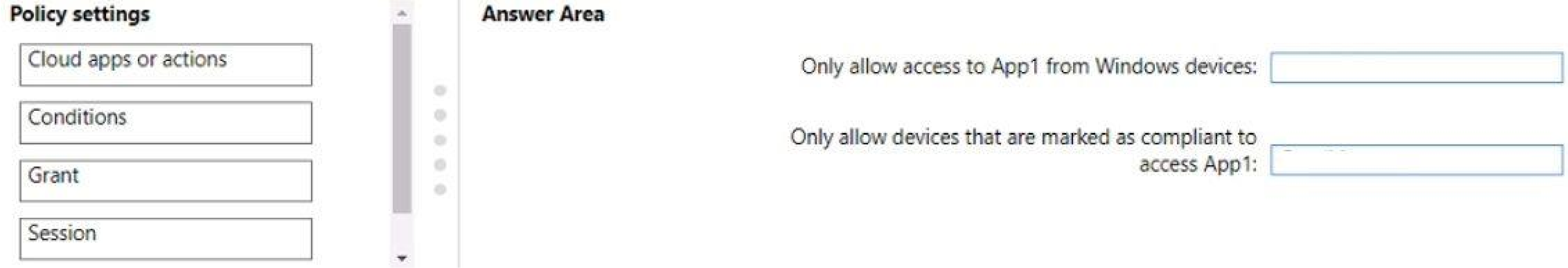
Resource group: RG2
- RG1
- RG2
- RG3

Subnet: AzureFirewallSubnet only
- AzureFirewall only
- AzureFirewallSubnet only
- AzureFirewall or AzureFirewallSubnet only
- AzureFirewall, AzureFirewallSubnet, or Subnet2 only
- AzureFirewall, AzureFirewallSubnet, Subnet1, or Subnet2

Section:
Explanation:

QUESTION 28
DRAG DROP
You have an Azure subscription that contains an Azure web app named Appl.
You plan to configure a Conditional Access policy for App1. The solution must meet the following requirements:
• Only allow access to App1 from Windows devices.
• Only allow devices that are marked as compliant to access App1.
Which Conditional Access policy settings should you configure? To answer, drag the appropriate settings to the correct requirements. Each setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.

Select and Place:



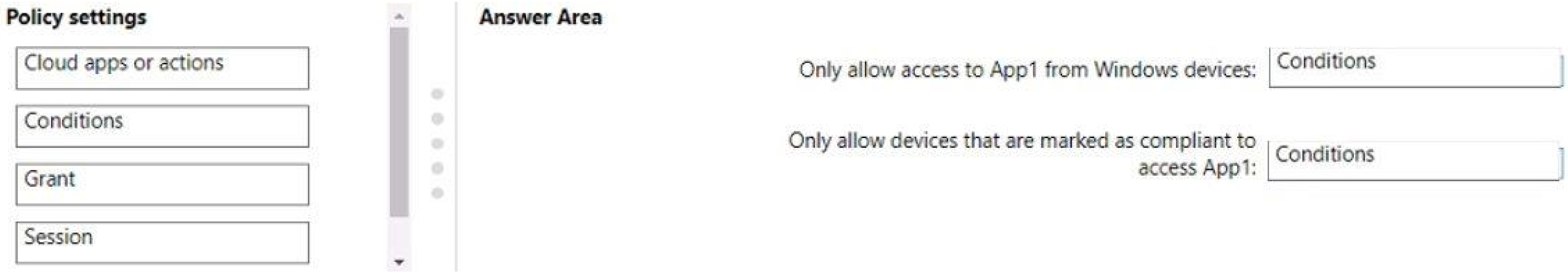
Policy settings
- Cloud apps or actions
- Conditions
- Grant
- Session

Answer Area

Only allow access to App1 from Windows devices:

Only allow devices that are marked as compliant to access App1:

Correct Answer:



Policy settings

- Cloud apps or actions
- Conditions
- Grant
- Session

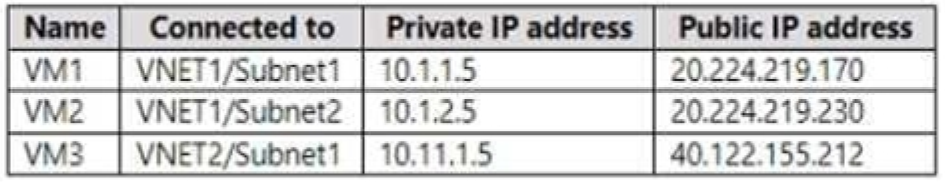
Answer Area

Only allow access to App1 from Windows devices: Conditions

Only allow devices that are marked as compliant to access App1: Conditions

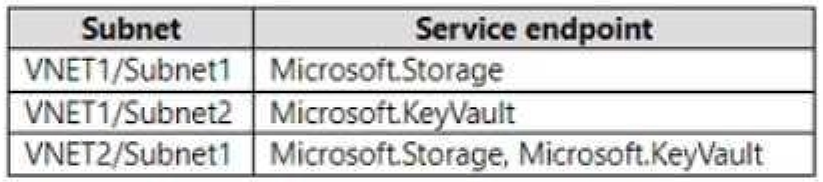
Section:
Explanation:

QUESTION 29
HOTSPOT
You have an Azure subscription that is linked to an Azure AD tenant and contains the virtual machines shown in the following table.



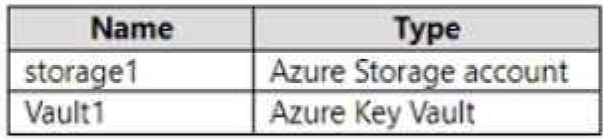
Name	Connected to	Private IP address	Public IP address
VM1	VNET1/Subnet1	10.1.1.5	20.224.219.170
VM2	VNET1/Subnet2	10.1.2.5	20.224.219.230
VM3	VNET2/Subnet1	10.11.1.5	40.122.155.212

The subnets of the virtual networks have the service endpoints shown in the following table.



Subnet	Service endpoint
VNET1/Subnet1	Microsoft.Storage
VNET1/Subnet2	Microsoft.KeyVault
VNET2/Subnet1	Microsoft.Storage, Microsoft.KeyVault

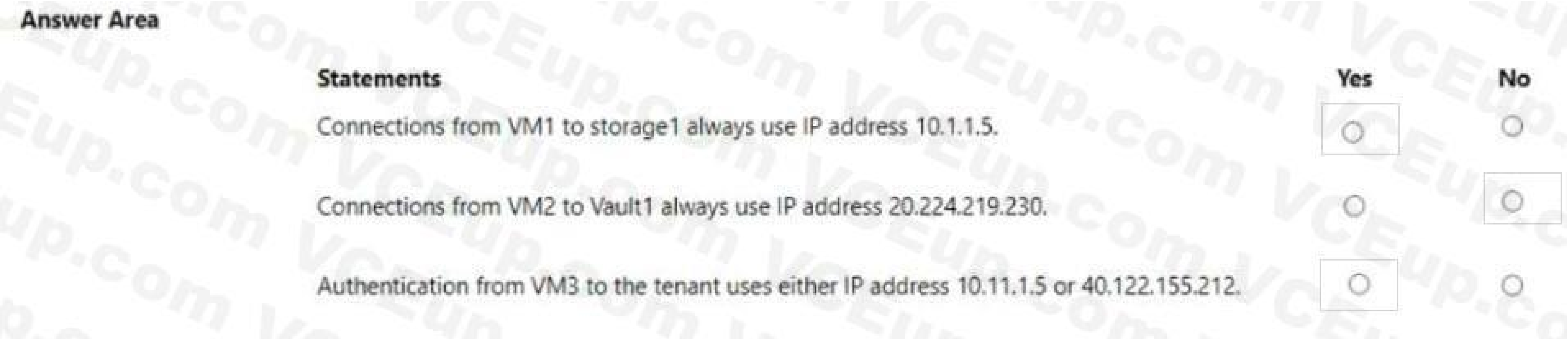
You create the resources shown in the following table.



Name	Type
storage1	Azure Storage account
Vault1	Azure Key Vault

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE:
Each correct selection is worth one point.

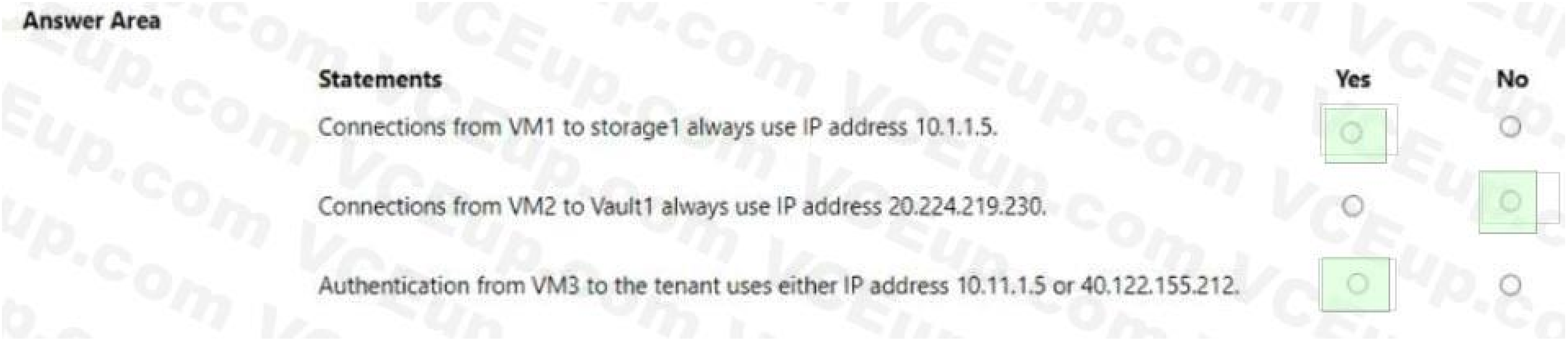
Hot Area:



Answer Area

Statements	Yes	No
Connections from VM1 to storage1 always use IP address 10.1.1.5.	○	○
Connections from VM2 to Vault1 always use IP address 20.224.219.230.	○	○
Authentication from VM3 to the tenant uses either IP address 10.11.1.5 or 40.122.155.212.	○	○

Answer Area:



Answer Area

Statements	Yes	No
Connections from VM1 to storage1 always use IP address 10.1.1.5.	[✓ ○]	○
Connections from VM2 to Vault1 always use IP address 20.224.219.230.	○	[✓ ○]
Authentication from VM3 to the tenant uses either IP address 10.11.1.5 or 40.122.155.212.	[✓ ○]	○

Section:
Explanation:

QUESTION 30
You have an Azure subscription that uses Microsoft Defender for Cloud.
You need to use Defender for Cloud to review regulatory compliance with the Azure CIS 1.4,0 standard. The solution must minimize administrative effort. What should you do first?

A. Assign an Azure policy.
B. Manually add the Azure CIS 1.4.0 standard.
C. Disable one of the Out of the box standards.
D. Add a custom initiative.

Correct Answer: A
Section:

QUESTION 31
You have an Azure subscription that contains a storage account named storage1 and a virtual machine named VM1. VM1 is connected to a virtual network named VNet1 that contains one subnet and uses Azure DNS.You need to ensure that VM1 connects to storage1 by using a private IP address. The solution must minimize administrative effort.What should you do?

A. For storage1, disable public network access.
B. Create an Azure Private DNS zone.
C. On VNet1. create a new subnet.
D. For storage1, create a new private endpoint.

Correct Answer: D
Section:

QUESTION 32
You have an Azure subscription that uses Microsoft Defender for Cloud.
You have an Amazon Web Service (AWS) account named AWS1 that is connected to defender for Cloud.
You need to ensure that AWS foundational Security Best Practices. The solution must minimize administrate effort.
What should do you in Defender for Cloud?

A. Create a new customer assessment.
B. Assign a built-in assessment.
C. Assign a built-in compliance standard.
D. Create a new custom standard.

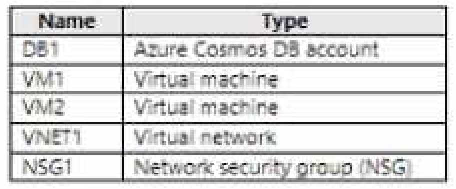
Correct Answer: C
Section:

QUESTION 33
You have an Azure subscription that contains an Azure Blob storage account bolb1.
You need to configure attribute-based access control (ABAC) for blob1.
Which attributes can you use in access conditions?

A. blob index tags only
B. blob index tags and container names only
C. file extensions and container names only
D. blob index tags, file extensions, and container names

Correct Answer: A
Section:

QUESTION 34
You have an Azure subscription that contains the resources show in the following table.



Name	Type
DB1	Azure Cosmos DB account
VM1	Virtual machine
VM2	Virtual machine
VNET1	Virtual network
NSG1	Network security group (NSG)

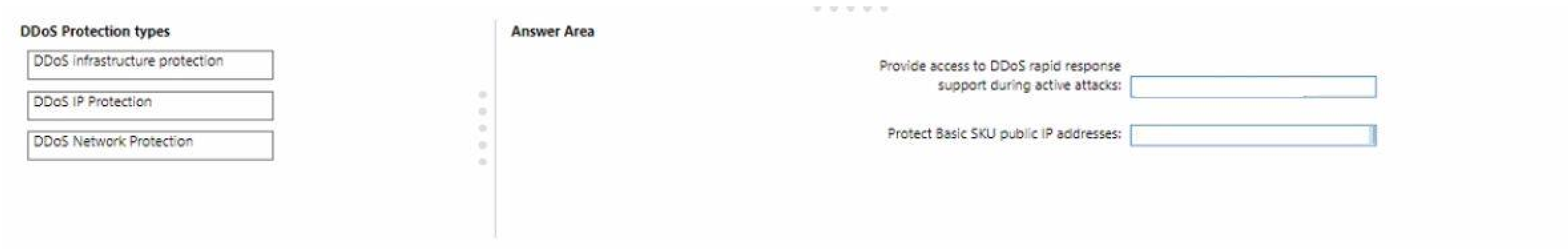
Both VM1 and VM2 connect to VNET1 and are configured to use NSG1.
You need to ensure that only VM1 and VM2 can access DB1.
What should you do?

A. Add the IP address range of VNET1 to the Firewall setting of DB1.
B. For NSG1, configure a rule that has a service tag.
C. Create an application security group.
D. Configure DB1 to allow access from only VNET1.

Correct Answer: B
Section:

QUESTION 35
DRAG DROP
You have an Azure subscription.
You plan to implement Azure DDoS Protection. The solution must meet the following requirement:
* Provide access to DDoS rapid response support during active attacks.
* Project Basic SKU public IP addresses.
You need to recommend which type of DDoS projection to use for each requirement.
What should you recommend? To answer, drag the appropriate DDoS projection types to the correct requirements. Each DDoS Projection type may be used once, or not at all. You may need to drag the split bar between panes or scroll to view connect.
NOTE: Each correct selection is worth one point.
Answer:

Select and Place:



DDoS Protection types

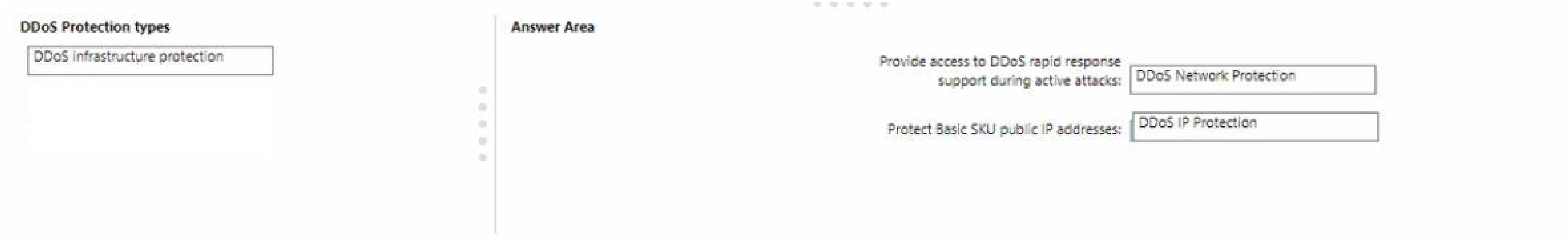
- DDoS infrastructure protection
- DDoS IP Protection
- DDoS Network Protection

Answer Area

Provide access to DDoS rapid response support during active attacks:

Protect Basic SKU public IP addresses:

Correct Answer:



DDoS Protection types

- DDoS infrastructure protection

Answer Area

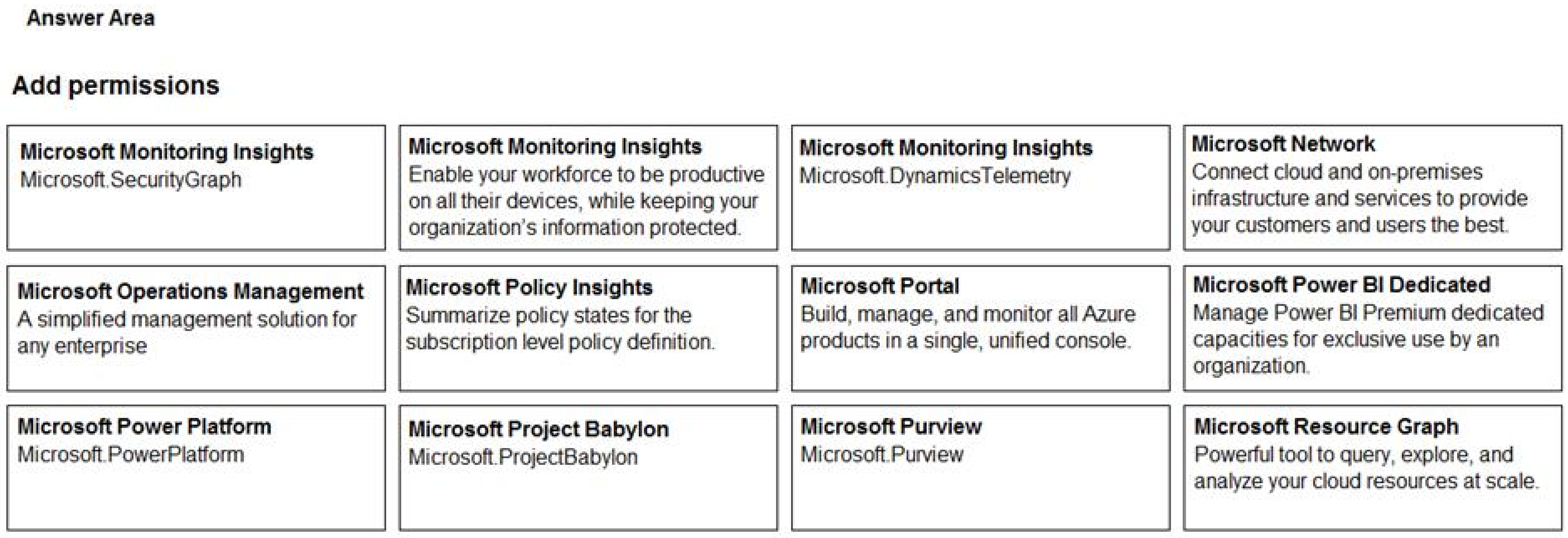
Provide access to DDoS rapid response support during active attacks: DDoS Network Protection

Protect Basic SKU public IP addresses: DDoS IP Protection

Section:
Explanation:

QUESTION 36
HOTSPOT
You have an Azure subscription that contains a user named User1. User1 is assigned the Reader role for the subscription.
You plan to create a custom role named Role1 and assign Role1 to User1.
You need to ensure that User1 can create and manage application security groups by using the Azure portal.
Which two permissions should you add to Role1? To answer, select the appropriate permission in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:

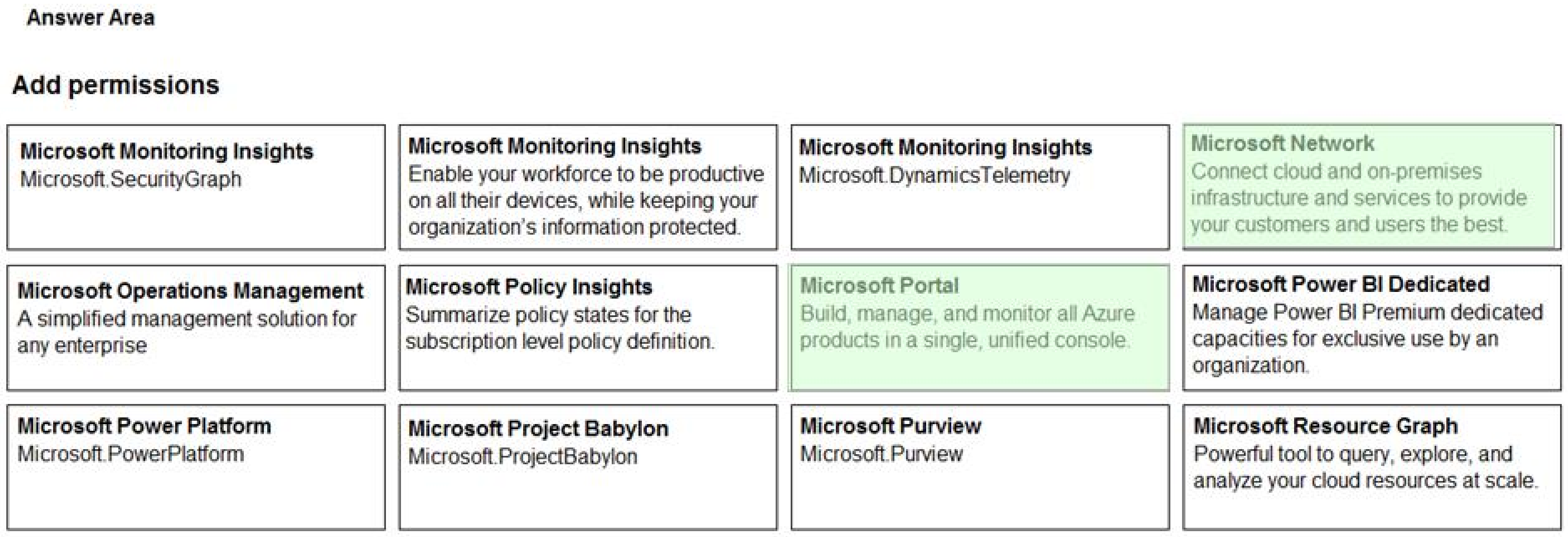


Answer Area

Add permissions

Microsoft Monitoring Insights Microsoft.SecurityGraph	**Microsoft Monitoring Insights** Enable your workforce to be productive on all their devices, while keeping your organization's information protected.	**Microsoft Monitoring Insights** Microsoft.DynamicsTelemetry	**Microsoft Network** Connect cloud and on-premises infrastructure and services to provide your customers and users the best.
Microsoft Operations Management A simplified management solution for any enterprise	**Microsoft Policy Insights** Summarize policy states for the subscription level policy definition.	**Microsoft Portal** Build, manage, and monitor all Azure products in a single, unified console.	**Microsoft Power BI Dedicated** Manage Power BI Premium dedicated capacities for exclusive use by an organization.
Microsoft Power Platform Microsoft.PowerPlatform	**Microsoft Project Babylon** Microsoft.ProjectBabylon	**Microsoft Purview** Microsoft.Purview	**Microsoft Resource Graph** Powerful tool to query, explore, and analyze your cloud resources at scale.

Answer Area:



Answer Area

Add permissions

Microsoft Monitoring Insights Microsoft.SecurityGraph	**Microsoft Monitoring Insights** Enable your workforce to be productive on all their devices, while keeping your organization's information protected.	**Microsoft Monitoring Insights** Microsoft.DynamicsTelemetry	**Microsoft Network** Connect cloud and on-premises infrastructure and services to provide your customers and users the best.
Microsoft Operations Management A simplified management solution for any enterprise	**Microsoft Policy Insights** Summarize policy states for the subscription level policy definition.	**Microsoft Portal** Build, manage, and monitor all Azure products in a single, unified console.	**Microsoft Power BI Dedicated** Manage Power BI Premium dedicated capacities for exclusive use by an organization.
Microsoft Power Platform Microsoft.PowerPlatform	**Microsoft Project Babylon** Microsoft.ProjectBabylon	**Microsoft Purview** Microsoft.Purview	**Microsoft Resource Graph** Powerful tool to query, explore, and analyze your cloud resources at scale.

Section:

Explanation:

1. Microsoft Portal
2. Microsoft Network https://learn.microsoft.com/en-us/azure/azure-resourcemanager/management/azure-services-resource-providers

QUESTION 37

You have an Azure Active Directory (Azure AD) tenant.You need to prevent nonprivileged Azure AD users from creating service principals in Azure AD.What should you do in the Azure Active Directory admin center of the tenant?

A. From the Properties Wade, set Enable Security defaults to Yes.

B. From the Properties blade, set Access management fen Azure resources to No

C. From the User settings blade, set Users can register applications to No

D. From the User settings blade, set Restrict access to Azure AD administration portal to Yes.

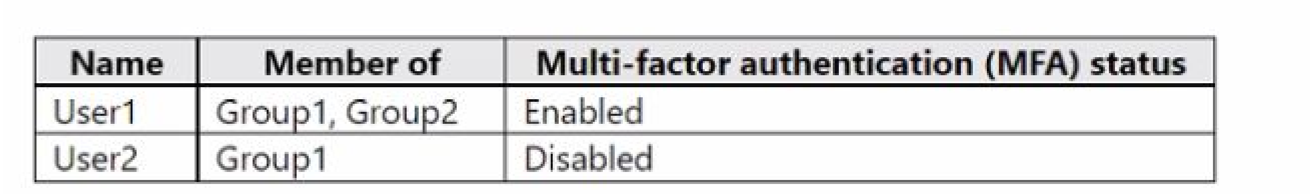
Correct Answer: C

Section:

QUESTION 38

HOTSPOT

You have a Microsoft Entra tenant that contains the users shown in the following table.



Name	Member of	Multi-factor authentication (MFA) status
User1	Group1, Group2	Enabled
User2	Group1	Disabled

You create and enforce a Microsoft Entra Identity Protection sign-in risk policy that has the following settings:

* Assignments: Include Group1, exclude Group2

* Conditions: Sign-in risk level: Low and above

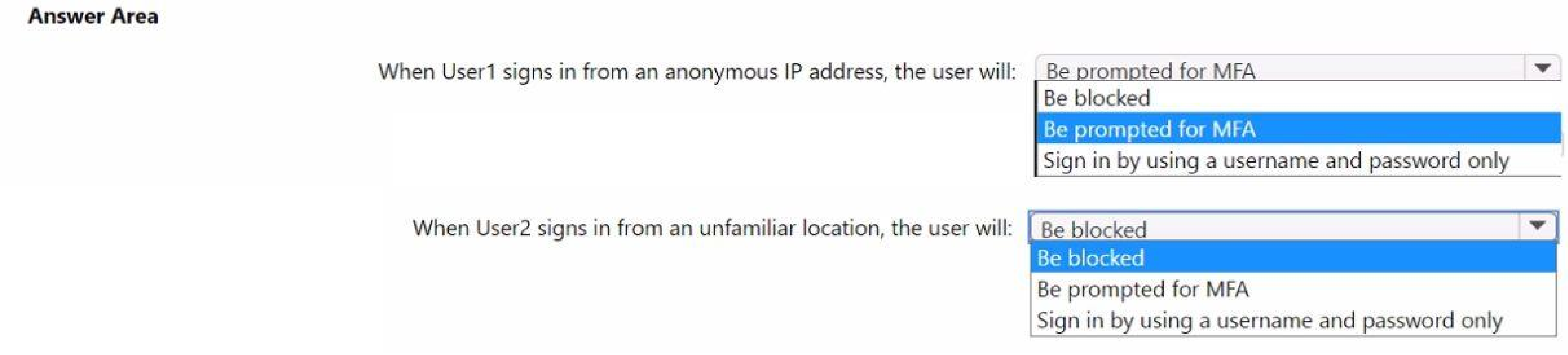
* Access: Allow access, Require multi-factor authentication

You need to identify what occurs when the users sign in to Microsoft Entra ID.

What should you identify for each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

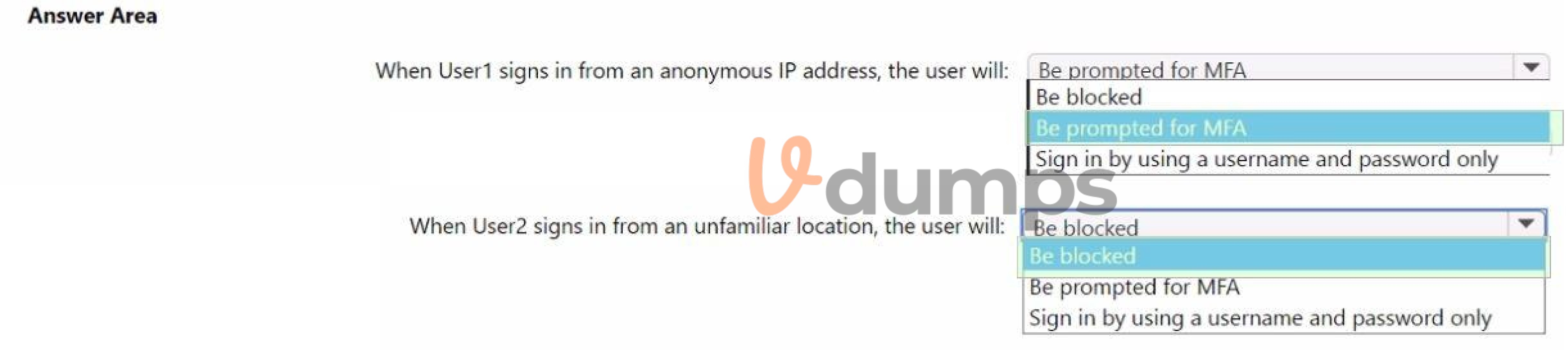
When User1 signs in from an anonymous IP address, the user will: Be prompted for MFA

- Be blocked
- Be prompted for MFA
- Sign in by using a username and password only

When User2 signs in from an unfamiliar location, the user will: Be blocked

- Be blocked
- Be prompted for MFA
- Sign in by using a username and password only

Answer Area:



Answer Area

When User1 signs in from an anonymous IP address, the user will: Be prompted for MFA

- Be blocked
- Be prompted for MFA
- Sign in by using a username and password only

When User2 signs in from an unfamiliar location, the user will: Be blocked

- Be blocked
- Be prompted for MFA
- Sign in by using a username and password only

Section:
Explanation:

QUESTION 39
You have a Microsoft Entra tenant that contains a user named User1.
You plan to enable passwordless authentication for the tenant.
You need to ensure that User1 can enable the combined registration experience. The solution must use the principle of least privilege.
Which role should you assign to User1?

A. Security Administrator
B. Global Administrator
C. Privileged Role Administrator
D. Authentication Administrator

Correct Answer: D
Section:

QUESTION 40

You have an Azure subscription that contains a virtual network named VNet1 VNet1 contains a single subnet. The subscription contains a virtual machine named VM1 that is connected to VNet1.
You plan to deploy an Azure SQL managed instance named SQL1.
You need to ensure that VM1 can access SQL1.
Which three components should you create? Each correct answer presents pan of the solution.
NOTE: Each correct selection is worth one point.

A. a virtual network gateway
B. a network security group (NSG)
C. a route table
D. a subnet
E. a network security perimeter

Correct Answer: B, C, D
Section: